

Scan Results

April 27, 2026

Report Summary	
User Name:	Jorge Vega
Login Name:	autrd3rv
Company:	AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES
User Role:	Manager
Address:	cr 13a 34-72 piso 8
City:	BOGOTA D.C.
Zip:	110311
Country:	Colombia
Created:	04/27/2026 at 05:04:55 AM (GMT-1100)
Launch Date:	04/24/2026 at 12:45:40 PM (GMT-1100)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1777074340.27247
Scanner Appliances:	ANPSGLQUAL01 (Scanner 15.0.1-1, Vulnerability Signatures 2.6.589-2)
Duration:	03:18:19
Title:	REQ-80762
Asset Groups:	Servidores por Demanda
IPs:	172.40.123.5
Excluded IPs:	-
FQDNs:	-
Options Profile:	Option_Profile_Search_Full

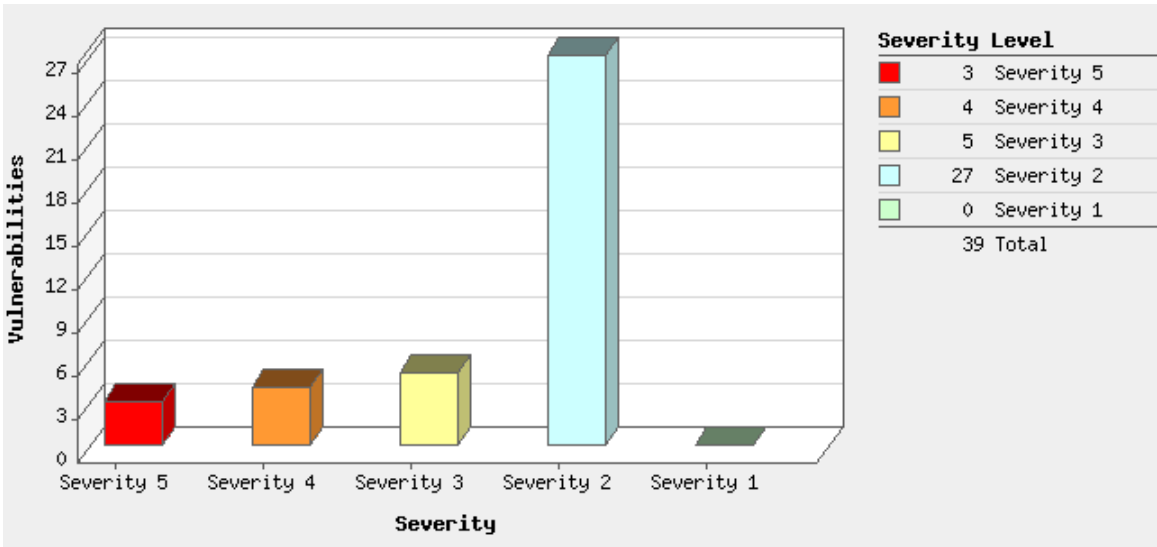
Summary of Vulnerabilities

Vulnerabilities Total	359	Security Risk (Avg)	5.0
-----------------------	-----	---------------------	---

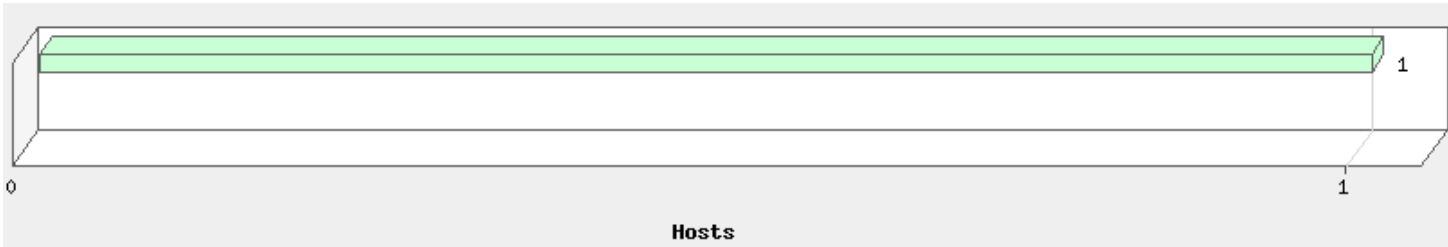
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	3	0	0	3
4	4	1	0	5
3	5	11	10	26
2	27	3	25	55
1	0	0	270	270
Total	39	15	305	359

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
General remote services	25	3	107	135
Information gathering	0	0	98	98
CGI	10	11	42	63
Web server	3	0	50	53
TCP/IP	0	0	7	7
Total	38	14	304	356

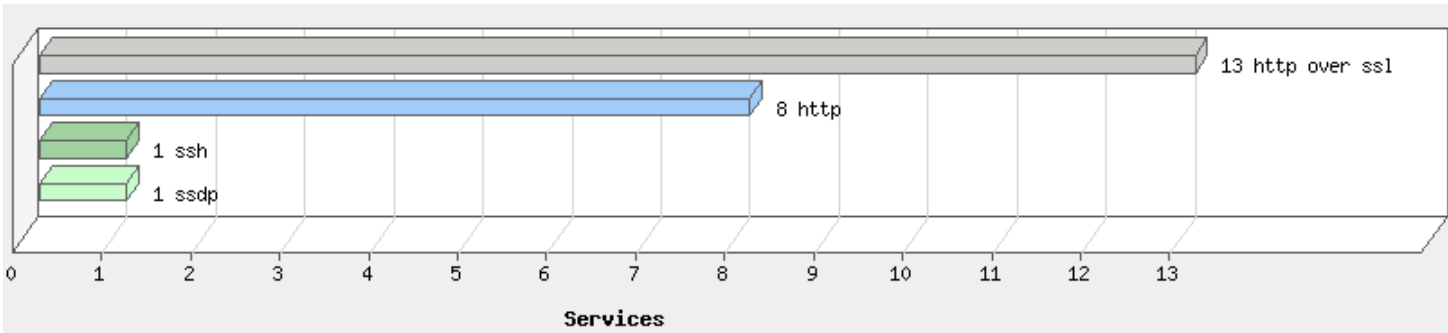
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

172.40.123.5 (-, -)

Vulnerabilities (39)

5 Flowise Arbitrary File Read Vulnerability

QID: 733275
Category: CGI
Associated CVEs: [CVE-2025-61913](#)
Vendor Reference: [GHSA-j44m-5v8f-gc9c](#)
Bugtraq ID: -

port 8000/tcp

Service Modified: 10/21/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

The ReadFileTool in Flowise does not restrict file path access, allowing authenticated attackers to exploit this vulnerability to read arbitrary files from the file system, potentially leading to remote command execution.

Affected Versions:
Flowise Versions up to 3.0.5 and including

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to Flowise 3.0.8 or later to address the vulnerability. For more information, please refer to the GHSA-j44m-5v8f-gc9c (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-j44m-5v8f-gc9c>)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
GHSA-j44m-5v8f-gc9c (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-j44m-5v8f-gc9c>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

 nist-nvd2

- Reference: CVE-2025-61913
Description: Flowise is a drag & drop user interface to build a customized large language model flow. In versions prior to 3.0.8, WriteFileTool and ReadFileTool in Flowise do not restrict file path access, allowing authenticated attackers to exploit this vulnerability to read and write arbitrary files to any path in the file system, potentially leading to remote command execution. Flowise 3.0.8 fixes this vulnerability.
Link: <https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-jv9m-vf54-chjj>
- Reference: CVE-2025-61913
Description: Flowise is a drag & drop user interface to build a customized large language model flow. In versions prior to 3.0.8, WriteFileTool and ReadFileTool in Flowise do not restrict file path access, allowing authenticated attackers to exploit this vulnerability to read and write arbitrary files to any path in the file system, potentially leading to remote command execution. Flowise 3.0.8 fixes this vulnerability.
Link: <https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-j44m-5v8f-gc9c>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Flowise detected on port 8000
GET /api/v1/version HTTP/1.1
Host: 172.40.123.5:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Connection: close

"version": "3.0.5"}

 5 Flowise Arbitrary File Read Vulnerability

port 3000/tcp

QID: 733275
Category: CGI

Associated CVEs: [CVE-2025-61913](#)
Vendor Reference: [GHSA-j44m-5v8f-gc9c](#)
Bugtraq ID: -
Service Modified: 10/21/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

The ReadFileTool in Flowise does not restrict file path access, allowing authenticated attackers to exploit this vulnerability to read arbitrary files from the file system, potentially leading to remote command execution.

Affected Versions:
Flowise Versions up to 3.0.5 and including

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to Flowise 3.0.8 or later to address the vulnerability. For more information, please refer to the [GHSA-j44m-5v8f-gc9c](https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-j44m-5v8f-gc9c) (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-j44m-5v8f-gc9c>)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[GHSA-j44m-5v8f-gc9c](https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-j44m-5v8f-gc9c) (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-j44m-5v8f-gc9c>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:



nist-nvd2

Reference: CVE-2025-61913

Description: Flowise is a drag & drop user interface to build a customized large language model flow. In versions prior to 3.0.8, WriteFileTool and ReadFileTool in Flowise do not restrict file path access, allowing authenticated attackers to exploit this vulnerability to read and write arbitrary files to any path in the file system, potentially leading to remote command execution. Flowise 3.0.8 fixes this vulnerability.

Link: <https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-jv9m-vf54-chjj>

Reference: CVE-2025-61913

Description: Flowise is a drag & drop user interface to build a customized large language model flow. In versions prior to 3.0.8, WriteFileTool and ReadFileTool in Flowise do not restrict file path access, allowing authenticated attackers to exploit this vulnerability to read and write arbitrary files to any path in the file system, potentially leading to remote command execution. Flowise 3.0.8 fixes this vulnerability.

Link: <https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-j44m-5v8f-gc9c>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Flowise detected on port 3000
GET /api/v1/version HTTP/1.1
Host: 172.40.123.5:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Connection: close

"version": "3.0.5"}

QID: 386998
 Category: Local
 Associated CVEs: [CVE-2025-57735](#), [CVE-2026-34538](#), [CVE-2025-66236](#), [CVE-2026-31987](#), [CVE-2026-32690](#), [CVE-2026-32228](#)
 Vendor Reference: [Airflow CVE-2025-66236](#), [Airflow CVE-2026-31987](#), [Airflow CVE-2025-57735](#), [Airflow CVE-2026-34538](#)
 Bugtraq ID: -
 Service Modified: 04/19/2026
 User Modified: -
 Edited: No
 PCI Vuln: Yes

THREAT:

CVE-2025-57735: When user logged out, the JWT token the user had authenticated with was not invalidated, which could lead to reuse of that token in case it was intercepted.

CVE-2026-34538: Authorization bypass in DagRun wait endpoint (XCom exposure)

CVE-2025-66236: Secrets from Airflow config file logged in plain text in DAG run logs UI

Affected Versions:
 Apache Airflow 3.0.0 before 3.2.0

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to Airflow 3.2.0 or later to patch the vulnerability. For more information, please refer to the Apache Airflow Advisory (<https://lists.apache.org/thread/ovn8mpd8zkc604hojt7x3wsw3kc60x98>) Apache Airflow Advisory (<https://lists.apache.org/thread/9mq3msqhmjgwdzbr6bgthj4brb3oz9fl>) Apache Airflow Advisory (<https://lists.apache.org/thread/g8fyy1tkmxkkfk7tx2v6h8mvwzpyykbo>)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Apache Security Advisory (<https://lists.apache.org/thread/ovn8mpd8zkc604hojt7x3wsw3kc60x98>)

Apache Security Advisory (<https://lists.apache.org/thread/9mq3msqhmjgwdzbr6bgthj4brb3oz9fl>)

Apache Security Advisory (<https://lists.apache.org/thread/g8fyy1tkmxkkfk7tx2v6h8mvwzpyykbo>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Apache Airflow Vulnerable version detected on 5002 port.

GET /api/v2/version HTTP/1.1

Host: 172.40.123.5:5002

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

Accept: */*

Connection: close

"version": "3.1.7", "git_version": ".dev0+83ff6ecec9dd71d8b8631248bc0725afc472acd7.dirty"}



QID: 732902
Category: CGI
Associated CVEs: [CVE-2025-8943](#), [CVE-2025-55346](#)
Vendor Reference: [GHSA-q4xx-mc3q-23x8](#), [GHSA-2vv2-3x8x-4gv7](#)
Bugtraq ID: -
Service Modified: 04/26/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

The Custom MCPs feature allows the execution of OS commands, such as using tools like npx to start local MCP Servers. However, Flowise has very limited authentication and authorization controls and does not support role-based access control (RBAC). In versions prior to 3.0.1, the default installation runs without authentication unless it is manually enabled. As a result, unauthenticated attackers on the network can execute unsandboxed OS commands.

Affected Versions:
Flowise 3.0.5 and prior versions

IMPACT:

This vulnerability allows unauthenticated attackers to run arbitrary OS commands on the server. Exploitation could lead to full system compromise, including data theft, service disruption, or further network attacks.

SOLUTION:

There are no patches as of now. For more information, please refer to [GHSA-2vv2-3x8x-4gv7](#) (<https://github.com/advisories/GHSA-2vv2-3x8x-4gv7>) and [GHSA-q4xx-mc3q-23x8](#) (<https://github.com/advisories/GHSA-q4xx-mc3q-23x8>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

metasploit

Reference: CVE-2025-8943

Description: Flowise Custom MCP Remote Code Execution

Link:

https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/http/flowise_custommcp_rce.rb



vulncheck-initial-access

Reference: CVE-2025-8943

Description: FlowiseAI Flowise CustomMCP Command Execution

Link:

<https://api.vulncheck.com/v3/index/initial-access?cve=CVE-2025-8943>



nist-nvd2

Reference: CVE-2025-8943

Description: The Custom MCPs feature is designed to execute OS commands, for instance, using tools like `npx` to spin up local MCP Servers. However, Flowise's inherent authentication and authorization model is minimal and lacks role-based access controls (RBAC). Furthermore, in Flowise versions before 3.0.1 the default installation operates without authentication unless explicitly configured. This combination allows unauthenticated network attackers to execute unsandboxed OS commands.

Link:

<https://research.jfrog.com/vulnerabilities/flowise-os-command-remote-code-execution-jfsa-2025-001380578/>



nuclei-templates

Reference: CVE-2025-8943

Description: Flowise < 3.0.1 - Remote Command Execution

Link:

<https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/main/http/cves/2025/CVE-2025-8943.yaml>



shadowserver-exploited

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-11-26&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-11-19&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-14&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-18&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-28&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-11-21&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-17&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-07&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-22&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-25&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-24&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-21&host_type=src&vulnerability=cv

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-16&host_type=src&vulnerability=cv

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-27&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-16&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-08&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-26&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-23&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-29&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-09&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-26&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-01&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-03&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-28&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-06&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)

Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-11&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-26&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-10&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-02&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-25&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-08&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-14&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-15&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-14&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-16&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-21&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-31&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-03&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-04&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-05&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-23&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-19&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-09&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-18&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-30&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-07&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-20&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-05&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-12&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-13&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)

Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-01&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-24&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-04&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-17&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-06&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-17&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-10&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-02&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-25&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-09&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-15&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-16&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-22&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-08&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-27&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-07&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-12&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-29&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-03&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-24&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-21&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-22&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-23&host_type=src&vulnerability=cve-2025-55346



vulncheck-threat-actors

Reference: CVE-2025-8943
Description: Unattributed
Link:

<https://app.crowdsec.net/cti/cve-explorer/CVE-2025-8943>

Reference: CVE-2025-8943
Description: Unattributed
Link:

<https://www.labs.greynoise.io/grimoire/2026-01-10-weekly-oast-report/>

Reference: CVE-2025-8943
Description: Unattributed
Link:

<https://www.labs.greynoise.io/grimoire/2026-02-13-weekly-oast-report/>

Reference: CVE-2025-8943
Description: Unattributed
Link: <https://www.linkedin.com/feed/update/urn:li:activity:7446686314562850817/>

? vulncheck-canaries

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-11-27>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-12-03>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-12-20>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-01-14>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-01-01>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-12-01>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-01-19>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-12-22>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-12-13>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-01-13>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-01-20>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-01-23>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-12-08>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-01-03>

Reference: CVE-2025-8943

[illegible]

[illegible]

[illegible]

[illegible]

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-03-21>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-03-20>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-09>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-08>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-07>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-06>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-05>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-04>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-03>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-02>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-01>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-03-31>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-03-30>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Flowise detected on port 8000
GET /api/v1/version HTTP/1.1
Host: 172.40.123.5:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Connection: close

"version": "3.0.5"}

QID:	733361
Category:	CGI
Associated CVEs:	CVE-2025-59528
Vendor Reference:	Flowise Security Advisory
Bugtraq ID:	-
Service Modified:	04/21/2026
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Flowise versions prior to 3.0.6 are vulnerable to remote code execution (RCE) via the /api/v1/node-load-method/customMCP endpoint. Authenticated users can exploit the loadMethod and mcpServerConfig parameters to execute arbitrary system commands on the host. This template performs a safe detection by sending a benign payload.

Affected Versions:
Flowise versions prior to 3.0.6

IMPACT:

Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code on the target system, leading to critical data loss and possible system compromise.

SOLUTION:

Customers are advised to upgrade to the latest version of Flowise to remediate this vulnerability. For more information, please refer to the Flowise Security Advisory (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-3gcm-f6qx-ff7p>).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
GHSA-3gcm-f6qx-ff7p (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-3gcm-f6qx-ff7p>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

exploitdb Reference: Description: Link: CVE-2025-59528 Flowise 3.0.4 - Remote Code Execution (RCE) https://www.exploit-db.com/exploits/52440
metasploit Reference: Description: Link: CVE-2025-59528 Flowise JS Injection RCE https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/http/flowise_js_rce.rb
github-exploits Reference: Description: Link: CVE-2025-59528 CVETeam/FlowiseAI-Critical-KillChain exploit repository https://github.com/CVETeam/FlowiseAI-Critical-KillChain
Reference: Description: Link: CVE-2025-59528 UsifAraby/CVE-2025-59528-POC exploit repository https://github.com/UsifAraby/CVE-2025-59528-POC
Reference: Description: CVE-2025-59528 kartik2005221/CVE-2025-58434-AND-59528-POC exploit repository

Link: <https://github.com/kartik2005221/CVE-2025-58434-AND-59528-POC>

Reference: CVE-2025-59528

Description: r3nsi15/Flowise-RCE-CVE-2025-59528 exploit repository

Link: <https://github.com/r3nsi15/Flowise-RCE-CVE-2025-59528>

Reference: CVE-2025-59528

Description: maradonam18/-CVE-2025-59528-PoC exploit repository

Link: <https://github.com/maradonam18/-CVE-2025-59528-PoC>

Reference: CVE-2025-59528

Description: TYehan/CVE-2025-58434-59528 exploit repository

Link: <https://github.com/TYehan/CVE-2025-58434-59528>

Reference: CVE-2025-59528

Description: vanhari/CVE-2025-59528 exploit repository

Link: <https://github.com/vanhari/CVE-2025-59528>

Reference: CVE-2025-59528

Description: danhle5402/CVE-2025-59528 exploit repository

Link: <https://github.com/danhle5402/CVE-2025-59528>

? vulncheck-initial-access

Reference: CVE-2025-59528

Description: FlowiseAI Flowise CustomMCP JS Code Injection

Link: <https://api.vulncheck.com/v3/index/initial-access?cve=CVE-2025-59528>

? nist-nvd2

Reference: CVE-2025-59528

Description: Flowise is a drag & drop user interface to build a customized large language model flow. In version 3.0.5, Flowise is vulnerable to remote code execution. The CustomMCP node allows users to input configuration settings for connecting to an external MCP server. This node parses the user-provided mcpServerConfig string to build the MCP server configuration. However, during this process, it executes JavaScript code without any security validation. Specifically, inside the convertToValidJSONString f

Link: <https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-3gcm-f6qx-ff7p>

? nuclei-templates

Reference: CVE-2025-59528

Description: Flowise - Remote Code Execution

Link: <https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/main/http/cves/2025/CVE-2025-59528.yaml>

? vulncheck-threat-actors

Reference: CVE-2025-59528

Description: Unattributed

Link: <https://www.linkedin.com/feed/update/urn:li:activity:7446686314562850817/>

? vulncheck-canaries

Reference: CVE-2025-59528

Description: VulnCheck Canaries CVE-2025-59528 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-14>

Reference: CVE-2025-59528

Description: VulnCheck Canaries CVE-2025-59528 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-13>

Reference: CVE-2025-59528

Description: VulnCheck Canaries CVE-2025-59528 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-10>

Reference: CVE-2025-59528

Description: VulnCheck Canaries CVE-2025-59528 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-12>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-11>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-07>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-06>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-09>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-08>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-05>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Flowise detected on port 8000
GET /api/v1/version HTTP/1.1
Host: 172.40.123.5:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Connection: close

```
"version": "3.0.5"}
```



4 Flowise Remote Code Execution (RCE) Vulnerability

port 3000/tcp

QID: 732902
Category: CGI
Associated CVEs: [CVE-2025-8943](#), [CVE-2025-55346](#)
Vendor Reference: [GHSA-q4xx-mc3q-23x8](#), [GHSA-2vv2-3x8x-4gv7](#)
Bugtraq ID: -
Service Modified: 04/26/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

The Custom MCPs feature allows the execution of OS commands, such as using tools like npx to start local MCP Servers. However, Flowise has very limited authentication and authorization controls and does not support role-based access control (RBAC). In versions prior to 3.0.1, the default installation runs without authentication unless it is manually enabled. As a result, unauthenticated attackers on the network can execute unsandboxed OS commands.

Affected Versions:
Flowise 3.0.5 and prior versions

IMPACT:

This vulnerability allows unauthenticated attackers to run arbitrary OS commands on the server. Exploitation could lead to full system compromise, including data theft, service disruption, or further network attacks.

SOLUTION:

There are no patches as of now. For more information, please refer to GHSA-2vv2-3x8x-4gv7 (<https://github.com/advisories/GHSA-2vv2-3x8x-4gv7>) and GHSA-q4xx-mc3q-23x8 (<https://github.com/advisories/GHSA-q4xx-mc3q-23x8>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

	metasploit
	Reference: CVE-2025-8943
	Description: Flowise Custom MCP Remote Code Execution
	Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/http/flowise_custommcp_rce.rb
	vulncheck-initial-access
	Reference: CVE-2025-8943
	Description: FlowiseAI Flowise CustomMCP Command Execution
	Link: https://api.vulncheck.com/v3/index/initial-access?cve=CVE-2025-8943
	nist-nvd2
	Reference: CVE-2025-8943
	Description: The Custom MCPs feature is designed to execute OS commands, for instance, using tools like `npx` to spin up local MCP Servers. However, Flowise's inherent authentication and authorization model is minimal and lacks role-based access controls (RBAC). Furthermore, in Flowise versions before 3.0.1 the default installation operates without authentication unless explicitly configured. This combination allows unauthenticated network attackers to execute unsandboxed OS commands.
	Link: https://research.jfrog.com/vulnerabilities/flowise-os-command-remote-code-execution-jfsa-2025-001380578/
	nuclei-templates
	Reference: CVE-2025-8943
	Description: Flowise < 3.0.1 - Remote Command Execution
	Link: https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/main/http/cves/2025/CVE-2025-8943.yaml
	shadowserver-exploited
	Reference: CVE-2025-55346
	Description: Flowise (CVE-2025-55346)
	Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-11-26&host_type=src&vulnerability=cve-2025-55346
	Reference: CVE-2025-55346
	Description: Flowise (CVE-2025-55346)
	Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-11-19&host_type=src&vulnerability=cve-2025-55346
	Reference: CVE-2025-55346
	Description: Flowise (CVE-2025-55346)
	Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-14&host_type=src&vulnerability=cve-2025-55346
	Reference: CVE-2025-55346
	Description: Flowise (CVE-2025-55346)
	Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-18&host_type=src&vulnerability=cve-2025-55346
	Reference: CVE-2025-55346
	Description: Flowise (CVE-2025-55346)
	Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-28&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-11-21&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-17&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-07&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-22&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-25&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-24&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-21&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-16&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-27&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-16&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-08&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-26&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)

Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-23&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-29&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2025-12-09&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-26&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-01&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-03&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-28&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-06&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-11&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-26&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-10&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-02&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-25&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-08&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-14&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-15&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-14&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-16&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-21&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-31&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-03&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-04&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-05&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-23&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-19&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)

Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-09&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-18&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-01-30&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-07&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-20&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-05&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-12&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-13&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-01&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-24&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-04&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-17&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link: https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-06&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-17&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-10&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-02&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-25&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-09&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-15&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-16&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-22&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-08&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-27&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-02-07&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)
Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-12&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346
Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-03-29&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-03&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-24&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-21&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-22&host_type=src&vulnerability=cve-2025-55346

Reference: CVE-2025-55346

Description: Flowise (CVE-2025-55346)

Link:

https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2026-04-23&host_type=src&vulnerability=cve-2025-55346



vulncheck-threat-actors

Reference: CVE-2025-8943

Description: Unattributed

Link: <https://app.crowdsec.net/cti/cve-explorer/CVE-2025-8943>

Reference: CVE-2025-8943

Description: Unattributed

Link: <https://www.labs.greynoise.io/grimoire/2026-01-10-weekly-oast-report/>

Reference: CVE-2025-8943

Description: Unattributed

Link: <https://www.labs.greynoise.io/grimoire/2026-02-13-weekly-oast-report/>

Reference: CVE-2025-8943

Description: Unattributed

Link: <https://www.linkedin.com/feed/update/urn:li:activity:7446686314562850817/>



vulncheck-canaries

Reference: CVE-2025-8943

Description: VulnCheck Canaries CVE-2025-8943 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-11-27>

Reference: CVE-2025-8943

Description: VulnCheck Canaries CVE-2025-8943 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-12-03>

Reference: CVE-2025-8943

Description: VulnCheck Canaries CVE-2025-8943 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2025-12-20>

Reference: CVE-2025-8943

Description: VulnCheck Canaries CVE-2025-8943 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-01-14>

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-06>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-05>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-04>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-03>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-02>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-04-01>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-03-31>

Reference: CVE-2025-8943
Description: VulnCheck Canaries CVE-2025-8943 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-8943&date=2026-03-30>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Flowise detected on port 3000
GET /api/v1/version HTTP/1.1
Host: 172.40.123.5:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Connection: close

"version": "3.0.5"}

4

Flowise Remote Code Execution (RCE) Vulnerability

port 3000/tcp

QID:

733361

Category:

CGI

Associated CVEs:

[CVE-2025-59528](#)

Vendor Reference:

[Flowise Security Advisory](#)

Bugtraq ID:

-

Service Modified:

04/21/2026

User Modified:

-

Edited:

No

PCI Vuln:

Yes

THREAT:

Flowise versions prior to 3.0.6 are vulnerable to remote code execution (RCE) via the /api/v1/node-load-method/customMCP endpoint. Authenticated users can exploit the loadMethod and mcpServerConfig parameters to execute arbitrary system commands on the host. This template performs a safe detection by sending a benign payload.

Affected Versions:
Flowise versions prior to 3.0.6

IMPACT:

Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code on the target system, leading to critical data loss and possible system compromise.

SOLUTION:

Customers are advised to upgrade to the latest version of Flowise to remediate this vulnerability. For more information, please refer to the Flowise Security Advisory (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-3gcm-f6qx-ff7p>).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

GHSA-3gcm-f6qx-ff7p (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-3gcm-f6qx-ff7p>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

 exploitdb

Reference: CVE-2025-59528

Description: Flowise 3.0.4 - Remote Code Execution (RCE)

Link: <https://www.exploit-db.com/exploits/52440>

 metasploit

Reference: CVE-2025-59528

Description: Flowise JS Injection RCE

Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/http/flowise_js_rce.rb

 github-exploits

Reference: CVE-2025-59528

Description: CVETeam/FlowiseAI-Critical-KillChain exploit repository

Link: <https://github.com/CVETeam/FlowiseAI-Critical-KillChain>

Reference: CVE-2025-59528

Description: UsifAraby/CVE-2025-59528-POC exploit repository

Link: <https://github.com/UsifAraby/CVE-2025-59528-POC>

Reference: CVE-2025-59528

Description: kartik2005221/CVE-2025-58434-AND-59528-POC exploit repository

Link: <https://github.com/kartik2005221/CVE-2025-58434-AND-59528-POC>

Reference: CVE-2025-59528

Description: r3nsi15/Flowise-RCE-CVE-2025-59528 exploit repository

Link: <https://github.com/r3nsi15/Flowise-RCE-CVE-2025-59528>

Reference: CVE-2025-59528

Description: maradonam18/-CVE-2025-59528-PoC exploit repository

Link: <https://github.com/maradonam18/-CVE-2025-59528-PoC>

Reference: CVE-2025-59528

Description: TYehan/CVE-2025-58434-59528 exploit repository

Link: <https://github.com/TYehan/CVE-2025-58434-59528>

Reference: CVE-2025-59528

Description: vanhari/CVE-2025-59528 exploit repository

Link: <https://github.com/vanhari/CVE-2025-59528>

Reference: CVE-2025-59528

Description: danhle5402/CVE-2025-59528 exploit repository
Link: <https://github.com/danhle5402/CVE-2025-59528>



vulncheck-initial-access

Reference: CVE-2025-59528
Description: FlowiseAI Flowise CustomMCP JS Code Injection
Link: <https://api.vulncheck.com/v3/index/initial-access?cve=CVE-2025-59528>



nist-nvd2

Reference: CVE-2025-59528
Description: Flowise is a drag & drop user interface to build a customized large language model flow. In version 3.0.5, Flowise is vulnerable to remote code execution. The CustomMCP node allows users to input configuration settings for connecting to an external MCP server. This node parses the user-provided mcpServerConfig string to build the MCP server configuration. However, during this process, it executes JavaScript code without any security validation. Specifically, inside the convertToValidJSONString f
Link: <https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-3gcm-f6qx-ff7p>



nuclei-templates

Reference: CVE-2025-59528
Description: Flowise - Remote Code Execution
Link: <https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/main/http/cves/2025/CVE-2025-59528.yaml>



vulncheck-threat-actors

Reference: CVE-2025-59528
Description: Unattributed
Link: <https://www.linkedin.com/feed/update/urn:li:activity:7446686314562850817/>



vulncheck-canaries

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-14>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-13>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-10>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-12>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-11>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-07>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-06>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation
Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-09>

Reference: CVE-2025-59528
Description: VulnCheck Canaries CVE-2025-59528 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-08>

Reference: CVE-2025-59528

Description: VulnCheck Canaries CVE-2025-59528 Exploitation

Link: <https://api.vulncheck.com/v3/index/vulncheck-canaries?cve=CVE-2025-59528&date=2026-04-05>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Flowise detected on port 3000
GET /api/v1/version HTTP/1.1
Host: 172.40.123.5:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Connection: close

```
"version": "3.0.5"}
```

3 Web Server Uses Plain-Text Form Based Authentication

port 8086/tcp

QID: 86728
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/24/2020
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.

IMPACT:

An attacker with access to the network traffic to and from the target host may be able to obtain login credentials for other users by sniffing the network traffic.

SOLUTION:

Please contact the vendor of the hardware/software for a possible fix for the issue. For custom applications, ensure that data sent via HTML login forms is encrypted before being sent from the client to the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /login HTTP/1.1
Host: 172.40.123.5:8086
Connection: Keep-Alive

```
<form method="post" name="login" action="_spring_security_check"><div><label class="app-sign-in-register__form-label"
for="_username">Username</label><input autocorrect="off" autocomplete="off" name="_username" id="_username" type="text"
autofocus="autofocus" class="jenkins-input " autocapitalize="off"></div><div><label class="app-sign-in-register__form-label"
for="_password">Password</label><input name="_password" id="_password" type="password" class="jenkins-input "></div><div
class="jenkins-checkbox"><input type="checkbox" id="remember_me" name="remember_me"><label for="remember_me">Keep me signed
in</label></div><input name="from" type="hidden"><input name="Jenkins-Crumb" type="hidden"
value="03eeeb28dc1cff21ff1159bf70aef1a43960a4e748c4f91fec6751b35514fabf"><button type="submit" name="Submit" class="jenkins-button
jenkins-button--primary">Sign in</button></form>
```

GET /login?next=/getting-started?next%3D/ HTTP/1.1
Host: 172.40.123.5:8086
Connection: Keep-Alive



3 FlowiseAI Command Injection Vulnerability

port 8000/tcp

QID: 733718
Category: CGI
Associated CVEs: [CVE-2025-57164](#)
Vendor Reference: [GHSA-7944-7c6r-55vv](#)
Bugtraq ID: -
Service Modified: 02/19/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

Flowise through v3.0.4 is vulnerable to remote code execution via unsanitized evaluation of user input in the "Supabase RPC Filter" field.

Affected Versions:
Flowise Versions up to 3.0.4 and including

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to Flowise 3.0.6 or later to address the vulnerability. For more information, please refer to the link here.
(<https://github.com/FlowiseAI/Flowise>)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

GHSA-7944-7c6r-55vv (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-7944-7c6r-55vv>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

 nist-nvd2

Reference: CVE-2025-57164

Description: Flowise through v3.0.4 is vulnerable to remote code execution via unsanitized evaluation of user input in the "Supabase RPC Filter" field.

Link: <https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-7944-7c6r-55vv>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Flowise detected on port 8000
GET /api/v1/version HTTP/1.1

Host: 172.40.123.5:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Connection: close

"version": "3.0.5"}

 3 FlowiseAI Command Injection Vulnerability

port 3000/tcp

QID: 733718
Category: CGI
Associated CVEs: [CVE-2025-57164](#)
Vendor Reference: [GHSA-7944-7c6r-55vv](#)
Bugtraq ID: -
Service Modified: 02/19/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

Flowise through v3.0.4 is vulnerable to remote code execution via unsanitized evaluation of user input in the "Supabase RPC Filter" field.

Affected Versions:
Flowise Versions up to 3.0.4 and including

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to Flowise 3.0.6 or later to address the vulnerability. For more information, please refer to the link here.
(<https://github.com/FlowiseAI/Flowise>)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
GHSA-7944-7c6r-55vv (<https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-7944-7c6r-55vv>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

 nist-nvd2
Reference: CVE-2025-57164
Description: Flowise through v3.0.4 is vulnerable to remote code execution via unsanitized evaluation of user input in the "Supabase RPC Filter" field.
Link: <https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-7944-7c6r-55vv>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Flowise detected on port 3000
GET /api/v1/version HTTP/1.1
Host: 172.40.123.5:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Connection: close

"version": "3.0.5"}

QID: 86728
 Category: Web server
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 08/24/2020
 User Modified: -
 Edited: No
 PCI Vuln: Yes

THREAT:

The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.

IMPACT:

An attacker with access to the network traffic to and from the target host may be able to obtain login credentials for other users by sniffing the network traffic.

SOLUTION:

Please contact the vendor of the hardware/software for a possible fix for the issue. For custom applications, ensure that data sent via HTML login forms is encrypted before being sent from the client to the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```

GET /auth/login/ HTTP/1.1
Host: 172.40.123.5:5002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: */*
Connection: close
  
```

```

<form class="form" action="" method="post" name="login">
  <input id="csrf_token" name="csrf_token" type="hidden"
value="IjlkMzM1YzcxMDQwYWU4YzllNGFiMzcwYmRkOGNINWVjMTE1ZGFiNjUi.aewllw.kHZXudWVrSbg67ida1nK4pVSiDk">
  <div class="help-block">Enter your login and password below:</div>
  <div class="control-group">
    <label class="control-label" for="username">Username:</label>

    <div class="controls">
      <div class="input-group">
        <span class="input-group-addon"><i class="fa fa-user"></i></span>
        <input autofocus class="form-control" id="username" name="username" required size="80" type="text" value="">
      </div>

      <label class="control-label" for="password">Password:</label>

      <div class="input-group">
        <span class="input-group-addon"><i class="fa fa-key"></i></span>
        <input class="form-control" id="password" name="password" required size="80" type="password" value="">
      </div>
    </div>
  </div>
</div>
  
```

```

<div class="control-group">
  <div class="controls">
    <br>
    <div>
      <input class="btn btn-primary btn-block" type="submit" value="Sign In">
    </div>
  </div>
</div>
</form>

```

GET /auth/login/ HTTP/1.1
Host: 172.40.123.5:5002
Connection: Keep-Alive



3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)

port 25000/tcp over SSL

QID: 38657
Category: General remote services
Associated CVEs: [CVE-2016-2183](#)
Vendor Reference: -
Bugtraq ID: 92630,95568
Service Modified: 12/15/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS

protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched

at following

versions

OPENSSL-0.9.8J-0.102.2
LIBOPENSSL0_9_8-0.9.8J-0.102.2
LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2
OPENSSL1-1.0.1G-0.52.1
OPENSSL1-DOC-1.0.1G-0.52.1
LIBOPENSSL1_0_0-1.0.1G-0.52.1
LIBOPENSSL1-DEVEL-1.0.1G-0.52.1
JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32 (<https://sweet32.info/>), Microsoft Windows

TLS changes docs (<https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server>) and

Microsoft Transport Layer Security (TLS) registry settings (<https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:



exploitdb

Reference: CVE-2016-2183

Description: IBM Informix Dynamic Server / Informix Open Admin Tool - DLL Injection / Remote Code Execution / Heap Buffer Overflow

Link: <https://www.exploit-db.com/exploits/42091>

? packetstorm
Reference: CVE-2016-2183
Description: IBM Informix Dynamic Server DLL Injection / Code Execution
Link: <https://packetstormsecurity.com/files/142756/IBM-Informix-Dynamic-Server-DLL-Injection-Code-Execution.html>

? 0day.today
Reference: CVE-2016-2183
Description: IBM Informix Dynamic Server / Informix Open Admin Tool - DLL Injection / Remote Code Execution / Hea
Link: <https://0day.today/exploit/27866>

Reference: CVE-2016-2183
Description: IBM Informix Dynamic Server / Informix Open Admin Tool - DLL Injection / Remote Code Execution / Hea
Link: <https://raw.githubusercontent.com/vulncheck-oss/0day.today.archive/main/web-applications/27866.txt>

? github-exploits
Reference: CVE-2016-2183
Description: ZakyHermawan/Simple-Sweet32 exploit repository
Link: <https://github.com/ZakyHermawan/Simple-Sweet32>

? nist-nvd2
Reference: CVE-2016-2183
Description: The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
Link: <https://www.exploit-db.com/exploits/42091/>

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM

2 SHA1 deprecated setting for SSH

port 22/tcp

QID: 38909
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/05/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another. The target is using deprecated SHA1 cryptographic settings to communicate.

IMPACT:

vulnerable to collision attacks, which are designed to fabricate the same hash value for different input data. each hash is supposedly unique.

SOLUTION:

Avoid using deprecated cryptographic settings.

Use best practices when configuring SSH.

Refer to NIST Retires SHA-1 Cryptographic Algorithm (SSH)

(<https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm>) .

Other documents to refer

Deprecate settings listed for red hat

(https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.4_release_notes/chap-red_hat_enterprise_linux-7.4_release_notes-deprecated_functionality_in_rhel7)

Key exchange (<https://www.ietf.org/archive/id/draft-ietf-curdle-ssh-kex-sha2-13.html>)

CBC Cipher (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5161>)

SHA1 ietf reference (<https://datatracker.ietf.org/doc/html/rfc9142>)

Settings currently considered deprecated:

1.Key exchange algorithms:

diffie-hellman-group1-sha1, rsa1024sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, gss-gex-sha1-*, gss-group1-sha1-* and gss-group14-sha1-*

2.MAC:

hmac-sha1, hmac-sha1-96, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com

3.Host key:

ssh-rsa, ssh-dss, ssh-rsa-cert-v01@openssh.com, ssh-dss-cert-v01@openssh.com

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Type	Name
MAC	hmac-sha1-etm@openssh.com
MAC	hmac-sha1

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 443/tcp over SSL

QID: 38170
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/05/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=Kubernetes_Ingress_Controller_Fake_Certificate,O=Acme_Co (ingress.local) doesn't resolve (Kubernetes Ingress Controller Fake Certificate) doesn't resolve



2 SSL Certificate - Signature Verification Failed Vulnerability

port 443/tcp over SSL

QID: 38173
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/18/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity with a Public Key and is used by clients to authenticate the server during an SSL/TLS connection. This authentication relies on verifying that the certificate is signed by a trusted Certificate Authority (CA).

If certificate verification fails, the client cannot reliably authenticate the server and may abort the connection or proceed without validation.

Verification failure may occur due to reasons such as a self-signed certificate, untrusted CA, missing intermediate certificates, expired or invalid certificates, mismatched issuer information, unsupported signature algorithms, or signature validation errors.

This may allow an attacker to perform man-in-the-middle attacks and compromise the confidentiality and integrity of the communication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Ensure the SSL certificate is valid and trusted. Install a certificate signed by a trusted Certificate Authority and configure the complete certificate chain, including any required intermediate certificates. Replace expired or invalid certificates and ensure proper issuer and signature configuration

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=Kubernetes_Ingress_Controller_Fake_Certificate,O=Acme_Co
ISSUER:_CN=Kubernetes_Ingress_Controller_Fake_Certificate,O=Acme_Co self signed certificate

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 10250/tcp over SSL

QID: 38170
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/05/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 O=system:nodes,CN=system:node:anqialazmv01 (anqialazmv01) doesn't resolve
(system:node:anqialazmv01) doesn't resolve

2 SSL Certificate - Signature Verification Failed Vulnerability

port 10250/tcp over SSL

QID: 38173
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/18/2026

User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity with a Public Key and is used by clients to authenticate the server during an SSL/TLS connection. This authentication relies on verifying that the certificate is signed by a trusted Certificate Authority (CA).

If certificate verification fails, the client cannot reliably authenticate the server and may abort the connection or proceed without validation.

Verification failure may occur due to reasons such as a self-signed certificate, untrusted CA, missing intermediate certificates, expired or invalid certificates, mismatched issuer information, unsupported signature algorithms, or signature validation errors.

This may allow an attacker to perform man-in-the-middle attacks and compromise the confidentiality and integrity of the communication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Ensure the SSL certificate is valid and trusted. Install a certificate signed by a trusted Certificate Authority and configure the complete certificate chain, including any required intermediate certificates. Replace expired or invalid certificates and ensure proper issuer and signature configuration

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 O=system:nodes,CN=system:node:anqialazmv01 ISSUER:_CN=10.152.183.1 unable to get local issuer certificate

 2 SSL Certificate - Invalid Maximum Validity Date Detected

port 10250/tcp over SSL

QID: 38685
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 04/13/2021
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

Subscriber Certificates issued on or after 1 September 2020 SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days. (13 months)

Subscriber Certificates issued after 1 March 2018, but prior to 1 September 2020, MUST NOT have a Validity Period greater than 825 days. (27 months)

Subscriber Certificates issued after 1 July 2016 but prior to 1 March 2018 MUST NOT have a Validity Period greater than 39 months.

SSL certificates have limited validity periods so that the certificate's holder identity information is re-authenticated more frequently. It is detected that maximum validity of certificate on the system is more than what is recommended.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate with recommended maximum validity.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 O=system:nodes,CN=system:node:anqialazmv01 ISSUER:_CN=10.152.183.1 is valid for more than 398 days



2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 8090/tcp over SSL

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/05/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.anla.gov.co,O=U_A_E_AUTORIDAD_NACIONAL_DE_LICENCIAS_AMBIENTALES_ANLA,ST=Distrito_Capital_de_Bogot,C=CO
(*anla.gov.co) doesn't resolve
(anla.gov.co) and IP (172.40.123.5) don't match
(*anla.gov.co) doesn't resolve



2 SSL Certificate - Self-Signed Certificate

port 8443/tcp over SSL

QID: 38169
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/23/2020
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=172.40.123.5,O=LocalDev,L=Bogota,ST=Cundinamarca,C=CO is a self signed certificate.



2 SSL Certificate - Improper Usage Vulnerability

port 8443/tcp over SSL

QID: 38172
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/15/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The basicConstraints section of the certificate may specify if it is a Certificate Authority (CA) certificate. Also, the keyUsage field in the X509v3 extensions section of the certificate, if present, may restrict the usage of the certificate.

In general, a server public key should not be used for Certificate or CRL signing, a client or CA certificate should be not used as a server certificate.

IMPACT:

If the keyUsage or the basicConstraint field is designated as a critical parameter in the certificate, the client may abort the communication if the usage validation fails.

SOLUTION:

Please install a server certificate with correct usage.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=172.40.123.5,O=LocalDev,L=Bogota,ST=Cundinamarca,C=CO is not suitable for CRL signing.



2 SSL Certificate - Signature Verification Failed Vulnerability

port 8443/tcp over SSL

QID:	38173
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2026
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity with a Public Key and is used by clients to authenticate the server during an SSL/TLS connection. This authentication relies on verifying that the certificate is signed by a trusted Certificate Authority (CA).

If certificate verification fails, the client cannot reliably authenticate the server and may abort the connection or proceed without validation.

Verification failure may occur due to reasons such as a self-signed certificate, untrusted CA, missing intermediate certificates, expired or invalid certificates, mismatched issuer information, unsupported signature algorithms, or signature validation errors.

This may allow an attacker to perform man-in-the-middle attacks and compromise the confidentiality and integrity of the communication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Ensure the SSL certificate is valid and trusted. Install a certificate signed by a trusted Certificate Authority and configure the complete certificate chain, including any required intermediate certificates. Replace expired or invalid certificates and ensure proper issuer and signature configuration

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=172.40.123.5,O=LocalDev,L=Bogota,ST=Cundinamarca,C=CO
ISSUER: _CN=172.40.123.5,O=LocalDev,L=Bogota,ST=Cundinamarca,C=CO self signed certificate



2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 9443/tcp over SSL

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/05/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 _ (localhost) doesn't resolve



2 SSL Certificate - Signature Verification Failed Vulnerability

port 9443/tcp over SSL

QID: 38173
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/18/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity with a Public Key and is used by clients to authenticate the server during an SSL/TLS connection. This authentication relies on verifying that the certificate is signed by a trusted Certificate Authority (CA).

If certificate verification fails, the client cannot reliably authenticate the server and may abort the connection or proceed without validation.

Verification failure may occur due to reasons such as a self-signed certificate, untrusted CA, missing intermediate certificates, expired or invalid certificates, mismatched issuer information, unsupported signature algorithms, or signature validation errors.

This may allow an attacker to perform man-in-the-middle attacks and compromise the confidentiality and integrity of the communication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Ensure the SSL certificate is valid and trusted. Install a certificate signed by a trusted Certificate Authority and configure the complete certificate chain, including any required intermediate certificates. Replace expired or invalid certificates and ensure proper issuer and signature configuration

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 __ self signed certificate



2 SSL Certificate - Invalid Maximum Validity Date Detected

port 9443/tcp over SSL

QID: 38685
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -

Service Modified: 04/13/2021
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

Subscriber Certificates issued on or after 1 September 2020 SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days. (13 months)
Subscriber Certificates issued after 1 March 2018, but prior to 1 September 2020, MUST NOT have a Validity Period greater than 825 days. (27 months)
Subscriber Certificates issued after 1 July 2016 but prior to 1 March 2018 MUST NOT have a Validity Period greater than 39 months.
SSL certificates have limited validity periods so that the certificate's holder identity information is re-authenticated more frequently.
It is detected that maximum validity of certificate on the system is more than what is recommended.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate with recommended maximum validity.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 __ is valid for more than 398 days

 2 HTTP Security Header Not Detected

port 9443/tcp

QID: 11827
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/02/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

This QID reports the absence of the following HTTP headers (https://www.owasp.org/index.php/OWASP_Secure-Headers_Project#tab=Headers) according to CWE-693: Protection Mechanism Failure (<https://cwe.mitre.org/data/definitions/693.html>):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.

Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -lL --verbose.

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Customers are advised to set proper X-Content-Type-Options (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>) and Strict-Transport-Security (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>) HTTP response headers.

Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:

X-Content-Type-Options:

Apache: Header always set X-Content-Type-Options: nosniff

HTTP Strict-Transport-Security:

Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

Nginx: add_header Strict-Transport-Security max-age=31536000;

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security HTTP Header missing on port 9443.

GET / HTTP/1.1

Host: 172.40.123.5:9443

Connection: Keep-Alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.1 200 OK

Accept-Ranges: bytes

Cache-Control: max-age=31536000

Content-Length: 19169

Content-Type: text/html; charset=utf-8

Last-Modified: Tue, 30 Apr 2024 22:47:07 GMT

Vary: Accept-Encoding

X-Content-Type-Options: nosniff

X-Csrf-Token:

X-Xss-Protection: 1; mode=block

Date: Sat, 25 Apr 2026 00:46:30 GMT



2 SSL Certificate - Self-Signed Certificate

port 8000/tcp over SSL

QID: 38169

Category: General remote services

Associated CVEs: -

Vendor Reference: -

Bugtraq ID: -

Service Modified: 11/23/2020

User Modified: -

Edited: No

PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=172.40.123.5,O=LocalDev,L=Bogota,ST=Cundinamarca,C=CO is a self signed certificate.

2 SSL Certificate - Improper Usage Vulnerability

port 8000/tcp over SSL

QID: 38172
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/15/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The basicConstraints section of the certificate may specify if it is a Certificate Authority (CA) certificate. Also, the keyUsage field in the X509v3 extensions section of the certificate, if present, may restrict the usage of the certificate.

In general, a server public key should not be used for Certificate or CRL signing, a client or CA certificate should be not used as a server certificate.

IMPACT:

If the keyUsage or the basicConstraint field is designated as a critical parameter in the certificate, the client may abort the communication if the usage validation fails.

SOLUTION:

Please install a server certificate with correct usage.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=172.40.123.5,O=LocalDev,L=Bogota,ST=Cundinamarca,C=CO is not suitable for CRL signing.

 2 SSL Certificate - Signature Verification Failed Vulnerability

port 8000/tcp over SSL

QID: 38173
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/18/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity with a Public Key and is used by clients to authenticate the server during an SSL/TLS connection. This authentication relies on verifying that the certificate is signed by a trusted Certificate Authority (CA).

If certificate verification fails, the client cannot reliably authenticate the server and may abort the connection or proceed without validation.

Verification failure may occur due to reasons such as a self-signed certificate, untrusted CA, missing intermediate certificates, expired or invalid certificates, mismatched issuer information, unsupported signature algorithms, or signature validation errors.

This may allow an attacker to perform man-in-the-middle attacks and compromise the confidentiality and integrity of the communication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Ensure the SSL certificate is valid and trusted. Install a certificate signed by a trusted Certificate Authority and configure the complete certificate chain, including any required intermediate certificates. Replace expired or invalid certificates and ensure proper issuer and signature configuration

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

 2 Session Cookie Does Not Contain the "Secure" Attribute

port 8081/tcp

QID: 13162
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/24/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

The secure cookie flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel.

A cookie with the secure attribute was not detected in the scan.

IMPACT:

Session cookies sent via HTTP expose users to sniffing attacks that could lead to user impersonation or account compromise.

SOLUTION:

Apply the "secure" attribute to session cookies to ensure that they are sent via HTTPS only. More information about this flag can be found here: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie>.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Cookie missing Secure attribute on port 8081.
Set-Cookie: pga4_session=58e6df27-f4b9-40f6-ac46-79ca8e03d6f9!6OkUcOs9EAoninVGWH/q0Ys/w7jOiYPHpb7JF/DD2Yw=; Expires=Sun, 26 Apr 2026 01:39:01 GMT; HttpOnly; Path=/; SameSite=Lax
GET / HTTP/1.1
Host: 172.40.123.5:8081
Connection: Keep-Alive

 2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication

port 5002/tcp

QID: 86729
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/28/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

Developers can add the following attribute to the form or input element: autocomplete="off"

This attribute prevents the browser from prompting the user to save the populated form values for later reuse.

Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera. However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.

Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /auth/login/ HTTP/1.1

Host: 172.40.123.5:5002

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

Accept: */*

Connection: close

```
<form class="form" action="" method="post" name="login">
  <input id="csrf_token" name="csrf_token" type="hidden"
value="IjlkMzM1YzcxMDQwYWU4YzllNGFiMzcwYmRkOGNINWVjMTE1ZGFjNjUi.aewllw.kHZXuWVrSbg67ida1nK4pVSIDk">
  <div class="help-block">Enter your login and password below:</div>
  <div class="control-group">
    <label class="control-label" for="username">Username:</label>

    <div class="controls">
      <div class="input-group">
        <span class="input-group-addon"><i class="fa fa-user"></i></span>
        <input autofocus class="form-control" id="username" name="username" required size="80" type="text" value="">
      </div>

      <label class="control-label" for="password">Password:</label>

      <div class="input-group">
        <span class="input-group-addon"><i class="fa fa-key"></i></span>
        <input class="form-control" id="password" name="password" required size="80" type="password" value="">
      </div>
    </div>
  </div>
  <div class="control-group">
    <div class="controls">
      <br>
    </div>
    <input class="btn btn-primary btn-block" type="submit" value="Sign In">
  </div>
</form>
```

</div>
</div>
</div>
</form>

GET /auth/login/ HTTP/1.1
Host: 172.40.123.5:5002
Connection: Keep-Alive

 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 9090/tcp over SSL

QID: 38170
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/05/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.anla.gov.co,O=U_A_E_AUTORIDAD_NACIONAL_DE_LICENCIAS_AMBIENTALES_ANLA,ST=Distrito_Capital_de_Bogot,C=CO
(*.anla.gov.co) doesn't resolve
(anla.gov.co) and IP (172.40.123.5) don't match
(*.anla.gov.co) doesn't resolve

 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 25000/tcp over SSL

QID: 38170
Category: General remote services

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/05/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=127.0.0.1,OU=Canonical,O=Canonical,L=Canonical,ST=Canonical,C=GB (kubernetes) doesn't resolve
(kubernetes.default) doesn't resolve
(kubernetes.default.svc) doesn't resolve
(kubernetes.default.svc.cluster) doesn't resolve
(kubernetes.default.svc.cluster.local) doesn't resolve
(127.0.0.1) and IP (172.40.123.5) don't match

2 SSL Certificate - Signature Verification Failed Vulnerability

port 25000/tcp over SSL

QID: 38173
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/18/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

An SSL Certificate associates an entity with a Public Key and is used by clients to authenticate the server during an SSL/TLS connection. This authentication relies on verifying that the certificate is signed by a trusted Certificate Authority (CA).

If certificate verification fails, the client cannot reliably authenticate the server and may abort the connection or proceed without validation.

Verification failure may occur due to reasons such as a self-signed certificate, untrusted CA, missing intermediate certificates, expired or invalid certificates, mismatched issuer information, unsupported signature algorithms, or signature validation errors.

This may allow an attacker to perform man-in-the-middle attacks and compromise the confidentiality and integrity of the communication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Ensure the SSL certificate is valid and trusted. Install a certificate signed by a trusted Certificate Authority and configure the complete certificate chain, including any required intermediate certificates. Replace expired or invalid certificates and ensure proper issuer and signature configuration

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=127.0.0.1,OU=Canonical,O=Canonical,L=Canonical,ST=Canonical,C=GB ISSUER:_CN=10.152.183.1 unable to get local issuer certificate

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 8089/tcp over SSL

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/05/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.anla.gov.co,O=U_A_E_AUTORIDAD_NACIONAL_DE_LICENCIAS_AMBIENTALES_ANLA,ST=Distrito_Capital_de_Bogot,C=CO
(*.anla.gov.co) doesn't resolve
(anla.gov.co) and IP (172.40.123.5) don't match
(*.anla.gov.co) doesn't resolve



2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 8093/tcp over SSL

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/05/2025
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.anla.gov.co,O=U_A_E_AUTORIDAD_NACIONAL_DE_LICENCIAS_AMBIENTALES_ANLA,ST=Distrito_Capital_de_Bogot,C=CO
(*.anla.gov.co) doesn't resolve
(anla.gov.co) and IP (172.40.123.5) don't match
(*.anla.gov.co) doesn't resolve

 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 9091/tcp over SSL

QID: 38170
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/05/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.anla.gov.co,O=U_A_E_AUTORIDAD_NACIONAL_DE_LICENCIAS_AMBIENTALES_ANLA,ST=Distrito_Capital_de_Bogot,C=CO
(*.anla.gov.co) doesn't resolve
(anla.gov.co) and IP (172.40.123.5) don't match
(*.anla.gov.co) doesn't resolve

 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 8088/tcp over SSL

QID: 38170
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/05/2025
User Modified: -
Edited: No

PCI Vuln: No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.anla.gov.co,O=U_A_E_AUTORIDAD_NACIONAL_DE_LICENCIAS_AMBIENTALES_ANLA,ST=Distrito_Capital_de_Bogot,C=CO
(*.anla.gov.co) doesn't resolve
(anla.gov.co) and IP (172.40.123.5) don't match
(*.anla.gov.co) doesn't resolve

 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN

port 8091/tcp over SSL

QID: 38170
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/05/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.anla.gov.co,O=U_A_E_AUTORIDAD_NACIONAL_DE_LICENCIAS_AMBIENTALES_ANLA,ST=Distrito_Capital_de_Bogot,C=CO
(*anla.gov.co) doesn't resolve
(anla.gov.co) and IP (172.40.123.5) don't match
(*anla.gov.co) doesn't resolve

Potential Vulnerabilities (15)



4 OpenSSH Authentication Bypass Vulnerability

QID: 38919
Category: General remote services
Associated CVEs: [CVE-2023-51767](#)
Vendor Reference: [OpenSSH 9.6](#)
Bugtraq ID: -
Service Modified: 04/19/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

In OpenSSH, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit.

Affected Versions:
OpenSSH up to version 9.6

IMPACT:

Successful exploitation allows OS command injection and row hammer attacks for authentication bypass.

SOLUTION:

There are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.15 detected on port 22 over TCP.

3 OpenSSH ssh Function Vulnerability (CVE-2025-61984)

QID: 38999
Category: General remote services
Associated CVEs: [CVE-2025-61984](#)
Vendor Reference: [openssh 10.1p1](#)
Bugtraq ID: -
Service Modified: 04/02/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

Affected Versions:
OpenSSH through version 10.1|10.1p1

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to OpenSSH 10.1p1 (<https://www.openssh.com/releasenotes.html#10.1p1>) or later to remediate this vulnerability.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[release-10.1p1 \(https://www.openssh.com/releasenotes.html#10.1p1\)](https://www.openssh.com/releasenotes.html#10.1p1)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

? github-exploits

Reference: CVE-2025-61984
Description: [dgl/cve-2025-61984-poc exploit repository](#)
Link: <https://github.com/dgl/cve-2025-61984-poc>

Reference: CVE-2025-61984
Description: [flyskyfire/cve-2025-61984-poc exploit repository](#)
Link: <https://github.com/flyskyfire/cve-2025-61984-poc>

? blogs

Reference: CVE-2025-61984
Description: [Bash a newline: Exploiting SSH via ProxyCommand, again \(CVE-2025-61984\)](#)
Link: https://dgl.cx/2025/10/bash-a-newline-ssh-proxycommand-cve-2025-61984#_

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.15 detected on port 22 over TCP.

QID: 732378
 Category: CGI
 Associated CVEs: [CVE-2024-7347](#)
 Vendor Reference: [NGINX Security Advisory](#)
 Bugtraq ID: -
 Service Modified: 09/05/2025
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A security issue was identified in the ngx_http_mp4_module, which might allow an attacker to cause a worker process crash by using a specially crafted mp4 file.

Affected Versions:

Nginx version from 1.5.13 prior to 1.26.2

Nginx version from 1.27.0 prior to 1.27.1

IMPACT:

Successful exploitation of the vulnerability allows an attacker to cause a worker process crash by using a specially crafted mp4 file .

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port: 8443 .

Server: nginx/1.25.4

Date: Sat, 25 Apr 2026 00:27:59 GMT

Content-Type: text/html

Content-Length: 479

Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT

Connection: keep-alive

ETag: "68c0f026-1df"

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Expires: 0

Access-Control-Allow-Origin: *

Access-Control-Allow-Credentials: true

Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS

Access-Control-Allow-Headers:

Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-Alive,Origin,User-Agent,X-Requested-With

Cross-Origin-Opener-Policy: same-origin

Cross-Origin-Embedder-Policy: require-corp

Accept-Ranges: bytes
<GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive

 3	Nginx Multiple Security Vulnerabilities (CVE-2024-31079,CVE-2024-32760,CVE-2024-34161,CVE-2024-35200)	port 8443/tcp
QID:	732379	
Category:	CGI	
Associated CVEs:	CVE-2024-31079 , CVE-2024-32760 , CVE-2024-34161 , CVE-2024-35200	
Vendor Reference:	NGINX Security Advisory	
Bugtraq ID:	-	
Service Modified:	03/27/2025	
User Modified:	-	
Edited:	No	
PCI Vuln:	Yes	

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

Multiple security issues were identified in nginx HTTP/3 implementation, which might allow an attacker that uses a specially crafted QUIC session to cause a worker process crash.

Affected Versions:

Nginx version from 1.25.0 to 1.25.5

Nginx version 1.26.0

IMPACT:

Successful exploitation of the vulnerabilities allows an attacker that uses a specially crafted QUIC session to cause a worker process crash

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to [NGINX Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[NGINX Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port: 8443 .

Server: nginx/1.25.4

Date: Sat, 25 Apr 2026 00:27:59 GMT

Content-Type: text/html

Content-Length: 479

Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT

Connection: keep-alive

ETag: "68c0f026-1df"

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Expires: 0

Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-Alive,Origin,User-Agent,X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

<GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive

 3 Nginx Buffer Overflow Vulnerability (CVE-2025-53859)

port 8443/tcp

QID: 732963
Category: CGI
Associated CVEs: [CVE-2025-53859](#)
Vendor Reference: [NGINX Security Advisory](#)
Bugtraq ID: -
Service Modified: 09/15/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.
A problem with SSL session resumption in nginx was identified.
Affected Versions:
Nginx versions 0.7.22-1.29.0

IMPACT:

Successful exploitation of the vulnerability allows certificate authentication bypass in some configurations

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to [NGINX Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port: 8443 .
Server: nginx/1.25.4
Date: Sat, 25 Apr 2026 00:27:59 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT

Connection: keep-alive
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

<GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive

3 NGINX SSL/TLS Upstream Injection Vulnerability (CVE-2026-1642)

port 8443/tcp

QID: 733929
Category: CGI
Associated CVEs: [CVE-2026-1642](#)
Vendor Reference: [NGINX Security Advisory](#)
Bugtraq ID: -
Service Modified: 04/02/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A vulnerability exists in NGINX when configured to proxy to upstream Transport Layer Security (TLS) servers. An attacker with a man-in-the-middle (MITM) position on the upstream server side along with conditions beyond the attacker's control may be able to inject plain text data into the response from an upstream proxied server.

Affected Versions:
Nginx versions 1.3.0-1.29.4

IMPACT:

Successful exploitation of this vulnerability could allow an attacker to inject plain text data into the response from an upstream proxied server.

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to [NGINX Security Advisory](#) (https://nginx.org/en/security_advisories.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port: 8443 .
Server: nginx/1.25.4
Date: Sat, 25 Apr 2026 00:27:59 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT
Connection: keep-alive
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

<GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive



3 Eclipse Jetty Memory Leak Vulnerability (CVE-2026-1605)

port 8086/tcp

QID: 733832
Category: CGI
Associated CVEs: [CVE-2026-1605](#)
Vendor Reference: [GHSA-xxh7-fcf3-rj7f](#)
Bugtraq ID: -
Service Modified: 03/12/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Eclipse Jetty is a Java HTTP server and Java Servlet container. While Web Servers are usually associated with serving documents to people, Jetty is now often used for machine to machine communications, usually within larger software frameworks.

Versions Affected:
Eclipse Jetty 12.0.0 to 12.0.31
Eclipse Jetty 12.1.0 to 12.1.5

IMPACT:

Successful exploitation of the vulnerability may lead to JVM to crash with OOME.

SOLUTION:

Customers are advised to refer to eclipse Jetty (<https://github.com/jetty/jetty.project/security/advisories/GHSA-xxh7-fcf3-rj7f>) for more information.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

GHSA-xxh7-fcf3-rj7f (<https://github.com/jetty/jetty.project/security/advisories/GHSA-xxh7-fcf3-rj7f>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Eclipse Jetty detected on port 8086 -

Server: Jetty(12.1.5)

Date: Fri, 24 Apr 2026 23:53:52 GMT

Vary: Accept-Encoding

X-Content-Type-Options: nosniff

Reporting-Endpoints: content-security-policy:

http://172.40.123.5:8086/content-security-policy-reporting-endpoint/J9P16uqZxjPB-hlp4-O2D0TgsOID0dTcMyrrhhVli6m8=:YW5vbnltb3Vz::Lw==

Content-Security-Policy-Report-Only: base-uri 'none'; default-src 'self'; form-action 'self'; frame-ancestors 'self'; img-src 'self' data::

script-src 'report-sample' 'self' usage.jenkins.io; style-src 'report-sample' 'self' 'unsafe-inline'; report-to content-security-policy;

report-uri http://172.40.123.5:8086/content-security-policy-reporting-endpoint/J9P16uqZxjPB-hlp4-O2D0TgsOID0dTcMyrrhhVli6m8=:YW5vbnltb3Vz::Lw==

Set-Cookie: JSESSIONID.9d431888=node0jshks9d7g6gb985xvgnc2ndq0.node0; Path=/; HttpOnly; SameSite=Lax

Expires: Thu, 01 Jan 1970 00:00:00 GMT

Content-Type: text/html;charset=utf-8

X-Hudson: 1.395

X-Jenkins: 2.541.3

X-Jenkins-Session: 24c0402b

<html><head><meta http-equiv='refr

3 Nginx Specially Crafted MP4 Vulnerability (CVE-2024-7347)

port 8443/tcp over SSL

QID: 732378

Category: CGI

Associated CVEs: [CVE-2024-7347](#)

Vendor Reference: [NGINX Security Advisory](#)

Bugtraq ID: -

Service Modified: 09/05/2025

User Modified: -

Edited: No

PCI Vuln: No

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A security issue was identified in the ngx_http_mp4_module, which might allow an attacker to cause a worker process crash by using a specially crafted mp4 file.

Affected Versions:

Nginx version from 1.5.13 prior to 1.26.2

Nginx version from 1.27.0 prior to 1.27.1

IMPACT:

Successful exploitation of the vulnerability allows an attacker to cause a worker process crash by using a specially crafted mp4 file .

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to [NGINX Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[NGINX Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port 8443 -
Server: nginx/1.25.4
Date: Fri, 24 Apr 2026 23:53:29 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT
Connection: close
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-Alive,Origin,User-Agent,X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>

<body>

  <script type="module">
    import Chatbot from "https://cdn.jsdelivr.net/npm/flowise-embed/dist/web.js"
    Chatbot.init({
```

3

Nginx Multiple Security Vulnerabilities (CVE-2024-31079,CVE-2024-32760,CVE-2024-34161,CVE-2024-35200)

port 8443/tcp over SSL

QID:	732379
Category:	CGI
Associated CVEs:	CVE-2024-31079 , CVE-2024-32760 , CVE-2024-34161 , CVE-2024-35200
Vendor Reference:	NGINX Security Advisory
Bugtraq ID:	-
Service Modified:	03/27/2025
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

Multiple security issues were identified in nginx HTTP/3 implementation, which might allow an attacker that uses a specially crafted QUIC session to cause a worker process crash.

Affected Versions:
Nginx version from 1.25.0 to 1.25.5
Nginx version 1.26.0

IMPACT:

Successful exploitation of the vulnerabilities allows an attacker that uses a specially crafted QUIC session to cause a worker process crash

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to [NGINX Security Advisory \(https://nginx.org/en/security_advisories.html\)](https://nginx.org/en/security_advisories.html)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port 8443 -
Server: nginx/1.25.4
Date: Fri, 24 Apr 2026 23:53:29 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT
Connection: close
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-Alive,Origin,User-Agent,X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>

<body>

  <script type="module">
    import Chatbot from "https://cdn.jsdelivr.net/npm/flowise-embed/dist/web.js"
    Chatbot.init({
```

3 Nginx Buffer Overflow Vulnerability (CVE-2025-53859)

port 8443/tcp over SSL

QID:	732963
Category:	CGI
Associated CVEs:	CVE-2025-53859
Vendor Reference:	NGINX Security Advisory
Bugtraq ID:	-
Service Modified:	09/15/2025
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A problem with SSL session resumption in nginx was identified.

Affected Versions:

Nginx versions 0.7.22-1.29.0

IMPACT:

Successful exploitation of the vulnerability allows certificate authentication bypass in some configurations

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port 8443 -

Server: nginx/1.25.4

Date: Fri, 24 Apr 2026 23:53:29 GMT

Content-Type: text/html

Content-Length: 479

Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT

Connection: close

ETag: "68c0f026-1df"

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Expires: 0

Access-Control-Allow-Origin: *

Access-Control-Allow-Credentials: true

Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS

Access-Control-Allow-Headers:

Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With

Cross-Origin-Opener-Policy: same-origin

Cross-Origin-Embedder-Policy: require-corp

Accept-Ranges: bytes

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>Document</title>

</head>

<body>

```
<script type="module">
  import Chatbot from "https://cdn.jsdelivr.net/npm/flowise-embed/dist/web.js"
  Chatbot.init({
```

3 NGINX SSL/TLS Upstream Injection Vulnerability (CVE-2026-1642)

port 8443/tcp over SSL

QID: 733929
Category: CGI
Associated CVEs: [CVE-2026-1642](#)
Vendor Reference: [NGINX Security Advisory](#)
Bugtraq ID: -
Service Modified: 04/02/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A vulnerability exists in NGINX when configured to proxy to upstream Transport Layer Security (TLS) servers. An attacker with a man-in-the-middle (MITM) position on the upstream server side along with conditions beyond the attacker's control may be able to inject plain text data into the response from an upstream proxied server.

Affected Versions:
Nginx versions 1.3.0-1.29.4

IMPACT:

Successful exploitation of this vulnerability could allow an attacker to inject plain text data into the response from an upstream proxied server.

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to [NGINX Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port 8443 -
Server: nginx/1.25.4
Date: Fri, 24 Apr 2026 23:53:29 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT
Connection: close
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true

Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-Alive,Origin,User-Agent,X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>

<body>

  <script type="module">
    import Chatbot from "https://cdn.jsdelivr.net/npm/flowise-embed/dist/web.js"
    Chatbot.init({
```



3 Apache Airflow Multiple Vulnerabilities (CVE-2025-54550)

port 5002/tcp

QID: 387092
Category: Local
Associated CVEs: [CVE-2025-54550](#), [CVE-2026-30912](#), [CVE-2026-30898](#), [CVE-2026-25917](#)
Vendor Reference: [Apache Airflow](#)
Bugtraq ID: -
Service Modified: 04/23/2026
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

CVE-2025-54550 : The example example_xcom that was included in airflow documentation implemented unsafe pattern of reading value from xcom in the way that could be exploited to allow UI user who had access to modify XComs to perform arbitrary execution of code on the worker

Affected Versions:
Apache Airflow prior to 3.2.0

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to Airflow 3.2.0 or later to patch the vulnerability. For more information, please refer to the Apache Airflow Advisory (<https://lists.apache.org/thread/3mf4cfx070ofsnf9qy0s2v5gqb5sc2g1>)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Security Advisory (<https://lists.apache.org/thread/3mf4cfx070ofsnf9qy0s2v5gqb5sc2g1>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Apache Airflow Vulnerable version detected on 5002 port.
GET /api/v2/version HTTP/1.1
Host: 172.40.123.5:5002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: */*
Connection: close

"version":"3.1.7","git_version":".dev0+83ff6ecec9dd71d8b8631248bc0725afc472acd7.dirty"}

 2 OpenSSH Expected Behavior Violation Vulnerability (CVE-2025-32728)

QID: 38979
Category: General remote services
Associated CVEs: [CVE-2025-32728](#)
Vendor Reference: [openssh 10.0](#)
Bugtraq ID: -
Service Modified: 04/06/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Affected Versions:OpenSSH before version 10.0

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to OpenSSH 10.0 (<https://www.openssh.com/txt/release-10.0>) or later to remediate this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[openssh 10.0 \(https://www.openssh.com/txt/release-10.0\)](https://www.openssh.com/txt/release-10.0)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.15 detected on port 22 over TCP.

 2 Nginx Certificate Authentication Bypass Vulnerability (CVE-2025-23419)

port 8443/tcp

QID: 732377
Category: CGI
Associated CVEs: [CVE-2025-23419](#)
Vendor Reference: [NGINX Security Advisory](#)

Bugtraq ID: -
Service Modified: 07/31/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.
A problem with SSL session resumption in nginx was identified.

Affected Versions:
Nginx version from 1.11.4 prior to 1.26.3
Nginx version from 1.27.0 prior to 1.27.4

IMPACT:

Successful exploitation of the vulnerability allows certificate authentication bypass in some configurations

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
NGINX Security Advisory (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port: 8443 .
Server: nginx/1.25.4
Date: Sat, 25 Apr 2026 00:27:59 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT
Connection: keep-alive
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

<GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive

QID: 732377
Category: CGI
Associated CVEs: [CVE-2025-23419](#)
Vendor Reference: [NGINX Security Advisory](#)
Bugtraq ID: -
Service Modified: 07/31/2025
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server.

A problem with SSL session resumption in nginx was identified.

Affected Versions:

Nginx version from 1.11.4 prior to 1.26.3

Nginx version from 1.27.0 prior to 1.27.4

IMPACT:

Successful exploitation of the vulnerability allows certificate authentication bypass in some configurations

SOLUTION:

Patch is also available, for more information about this vulnerability please refer to [NGINX Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[NGINX Security Advisory](https://nginx.org/en/security_advisories.html) (https://nginx.org/en/security_advisories.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Nginx detected on port 8443 -

Server: nginx/1.25.4

Date: Fri, 24 Apr 2026 23:53:29 GMT

Content-Type: text/html

Content-Length: 479

Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT

Connection: close

ETag: "68c0f026-1df"

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Expires: 0

Access-Control-Allow-Origin: *

Access-Control-Allow-Credentials: true

Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS

Access-Control-Allow-Headers:

Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With

Cross-Origin-Opener-Policy: same-origin

Cross-Origin-Embedder-Policy: require-corp

Accept-Ranges: bytes

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>

<body>

  <script type="module">
    import Chatbot from "https://cdn.jsdelivr.net/npm/flowise-embed/dist/web.js"
    Chatbot.init({
```

Information Gathered (305)

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/20/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: SSH on TCP port 22.

3 DEFLATE Data Compression Algorithm Used for HTTPS

QID:	42416
Category:	General remote services

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/09/2013
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.

DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.

This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Last-Modified: Tue, 30 Apr 2024 22:47:07 GMT
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Csrftoken:
X-Xss-Protection: 1; mode=block
Date: Sat, 25 Apr 2026 02:41:30 GMT
Transfer-Encoding: chunked

800

_1F_8B_08_00_00_00_00_00_FF_EC_BC_F9s_A3L_927_FE_FB_FE_15_1A_ED_C6_F6Lxlq_E9z_A6_DD_DF@K_C8_14_18_81,_A3_DD_FDF
@_08_84_0E_0B0_C7_EE_FE_EFodV_C9W_F7_D3_D3_CF_C6_1B_FB_C3_1B_E3_8E6_14_D4_91_95_C7'_B3_AA_12_7F_FDSp_F4_F3_FA_14_B6
_B6_F9>_FD_F6_15~_B7R_EF_10_DD_B6_C3C_BB_u_88_AE_BD_D3_E9_B6):_9Es/>_84gl_94_E5_E7_D8_CF_AF_83_B8_15x_B9w_1D_06q_1E_
1F_0F_B7me_DC_FE_F6u_1Bz_C1_B7_AF_FB0_F7Z_FE_D6:ga~_DB_.F2_CD_F5_A0_DD_F9_F65_8F_F34_FC_F6p_E9_EDk_87>_A0_D5_0F_DE>
_BCm_07a_E6_9F_E3_13_F4_D8n_F9_C7C_1E_1E_F2_DB64~W_C9+_F2_ED_F1_FC_EE_FDK_977_F1_F1_B5_EE6_CFO_D7_E1s_11_BF_DC_B6).
CF_DF_86_D7P_FF|L_DF5<_1C_AF_F1_D5_0F_1B_85_D5)>_87_D9_BB_EA_DC_0F_EB_9D_CE^_B4_F7~_D6+%_FB|_1F_F3_ECC_BD_F8_10_84
_15T[{Y_D8_8A_83_DB6_DC_C0_03_CA_86o_F1_A6_F5_E72>_04_C7_F2_E6x_8E_A3_F8_D0_BA_BDm}_D9_C4i_F8[_A7_F3_E5/_AD_FF_FC_A
7_16_FB_E9tZe_D8_F2_CEA+=zA|_88Z_F96ly_A7Sks>_EE[^+=_FA^_DA_82_A6-/k_C5_87Vp_F4w_E1_B9_15Vyx_C8_E2_E3_E1_B5_AB_E0_E
8_17_FB_F0_90_DFDa>NC_B8_1D_D5Z_F0_E7/@_DC_97_BF_DCl_CF_E1_A6u_DB_FA_02L_F8_AD_D3_C1_8E_B7_C7_FFM_1Ar_1C_D7_F9_F2_
B7_7Fz_ED_8A_D1_1E_04_E3_CB(AD_DBV~_.C2_BF_B1*_FF_DD
_D3[,7_8F_17_EF_DC:y_F9_B6u(i_0C_FD_83B_DC_C0c`_E5_CD9<_A5_9E_1F_FE_B9_F3_FF_FF{E7_EA_BF_FE_BDs_F5/_9D_E8_AF_AD/_
FE_F2_B7_0F_DD_00_B9_0F_B4+_EC_F1_FFK}_E9|j}_D1_C2_15_16~_83_DF_7F_FB_A33_BFt_FC:_89_AF_1D&_AF_AF_7F_BA_BE_FE_B7x_D
3J_F3_966n_FF_E3_1B_AB_C1_E4_D9_CA_CE_FEm_BB_D3_01C_EBf_Dbx_7F_13_1D_8FQ_1A_FA_C7
_BC_F1_8F_FBN_F6r_E8_E4_E7_E2_B0_A3Un_92_AC_FD_ED_B5s_EC_EB_EB_9F_FE<_04_F1_E6?_AE_AF_BF}M_E3_C3_AEu_0E_D3_DB_B6w:
_A5_E1u~_FC_EDu_EC_83_F5dq_13f_B7m~_C0U_FC_80k_B7_80_F6_DbvO_F4D_8E_Dfp_DD_BE_B4_E1_BD_DE_B0_E7_87_BD_9B_D3!_02_9D
{_EB_8D_F6_00_C8p_DB_8E_F7^_14v_A0_CA_A5KQ_A8D_E1_D2_A1_10_F8_1B_BF+_F4_03_AE_D7_0F\$/_14%A_FA_A3_1D_F2_BD_8A_EF]:_E

4y_C1_93_FAC_9F_1B_8A_1B_A9/_0C_85_1F|_DF_E1_DE_CBv|_A2_B4_19_80_D1o_B4_EB_EC%_BA_AA_F6_E9_DF@L=_E9_AF_0FSCX_D5#a_F54k_BC_E5_B0x_B0_B5J_8BG_D2zY_15~_C3_C5_De|_CE_F9_EA_F1E_17_031_A8_BB"

HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Content-Encoding: deflate
Content-Type: text/html; charset=utf-8
Last-Modified: Tue, 30 Apr 2024 22:47:07 GMT
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Csrft-Token:
X-Xss-Protection: 1; mode=block
Date: Sat, 25 Apr 2026 02:41:31 GMT
Transfer-Encoding: chunked

800
_EC_BC_F9s_A3L_927_FE_FB_FE_15_1A_ED_C6_F6Lxlq_E9z_A6_DD_DF@_K_C8_14_18_81_A3_DD_FDF
@_08_84_0E_0B0_C7_EE_FE_EFodV_C9W_F7_D3_D3_CF_C6_1B_FB_C3_1B_E3_8E6_14_D4_91_95_C7'_B3_AA_12_7F_FDSp_F4_F3_FA_14_B6
_B6_F9>_FD_F6_15~_B7R_EF_10_DD_B6_C3C_BBu_88_AE_BD_D3_E9_B6j: 9Es/>_84g|_94_E5_E7_D8_CF_AF_83_B8_15x_B9w_1D_06q_1E_
1F_0F_B7me_DC_FE_F6u_1Bz_C1_B7_AF_FB0_F7Z_FE_D6;ga~_DB_ F2_CD_F5_A0_DD_F9_F65_8F_F34_FC_F6p_E9_EDk_87>_A0_D5_0F_DE>
_BCm_07a_E6_9F_E3_13_F4_D8n_F9_C7C_1E_1E_F2_DB64~W_C9+ F2_ED_F1_FC_EE_FDK_977_F1_F1_B5_EE6_CFO_D7_E1s_11_BF_DC_B6j_
CF_DF_86_D7P_FF|L_DF5<_1C_AF_F1_D5_0F_1B_85_D5>_87_D9_BB_EA_DC_0F_EB_9D_CE^_B4_F7~_D6+%_FB|_1F_F3_ECC_BD_F8_10_84
_15T|{Y_D8_8A_83_DB6_DC_C0_03_CA_86o_F1_A6_F5_E72>_04_C7_F2_E6x_8E_A3_F8_D0_BA_BDm} D9_C4i_F8|_A7_F3_E5/_AD_FF_FC_A
7_16_FB_E9tZe_D8_F2_CEA+=zA|_88Z_F96ly_A7Sks>_EE[^+=_FA^_DA_82_A6/~k_C5_87Vp_F4w_E1_B9_15Vyx_C8_E2_E3_E1_B5_AB_E0_E
8_17_FB_F0_90_DFDa>NC_B8_1D_D5Z_F0_E7|/_DC_97_BF_DCl_CF_E1_A6u_DB_FA_02L_F8_AD_D3_C1_8E_B7_C7_FFM_1Ar_1C_D7_F9_F2_
B7_7Fz_ED_8A_D1_1E_04_E3_CB(_AD_DBV~_C2_BF_B1*_FF_DD
_D3|7_8F_17_EF_DC:y_F9_B6u|i_0C_FD_83B_DC_C0c'_E5_CD9<_A5_9E_1F_FE_B9_F3_FF_FF{_E7_EA_BF_FE_BDs_F5/_9D_E8_AF_AD/_
FE_F2_B7_0F_DD_00_B9_0F_B4+_EC_F1_Ffk} E9|j|_D1_C2_15_16~_83_DF_7F_FB_A33_Bf|_FC: 89_AF_1D&_AF_AF_7F_BA_BE_FE_B7x_D
3J_F3_966n_FF_E3_1B_AB_C1_E4_D9_CA_CE_FEm_BB_D3_01C_EBf_Dbx_7F_13_1D_8FQ_1A_FA_C7
_BC_F1_8F_FBN_F6r_E8_E4_E7_E2_B0_A3Un_92_AC_FD_ED_B5s_EC_EB_EB_9F_FE<_04_F1_E6?_AE_AF_Bf}M_E3_C3_AEu_0E_D3_DB_B6w:
_A5_E1u~, _FC_EDu_EC_83_F5dq_13f_B7m~_C0U_FC_80k_B7_80_F6_DBvO_F4D_8E_DFp_DD_BE_B4_E1_BD_DE_B0_E7_87_BD_9B_D3!_02_9D
{_EB_8D_F6_00_C8p_DB_8E_F7^_14v_A0_CA_A5KQ_A8D_E1_D2_A1_10_F8_1B_BF+_F4_03_AE_D7_0F\$/_14%A_FA_A3_1D_F2_BD_8A_EF|:_E
4y_C1_93_FAC_9F_1B_8A_1B_A9/_0C_85_1F|_DF_E1_DE_CBv|_A2_B4_19_80_D1o_B4_EB_EC%_BA_AA_F6_E9_DF@L=_E9_AF_0FSCX_D5#a_
F54k_BC_E5_B0x_B0_B5J_8BG_D2zY_15~_C3_C5_De|_CE_F9_EA_F1E_17_031_A8_BB"_A9_BB/_FE_DE_7F!

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:41:35 GMT
Content-Type: text/html
Last-Modified: Fri, 24 Apr 2026 20:28:05 GMT
Transfer-Encoding: chunked
Connection: keep-alive
ETag: W/"69ebd255-1d7"
Content-Encoding: gzip

133
_1F_8B_08_00_00_00_00_04_03e_91MO_C30_0C_86_EF_FB_15!Wh_03_12_A0_1D_9A_9E_D0nHH_83_1F_10_12_AF5_E4c_C4Y_F7_F1_EB
q_D7_A2_818_C5_89_?_B6_DF4W_D9r_DC_82_E8K_F0_ED_A2_19_0F_E1M_EC_B4_84(_DB_85_10M_0F_C6_8D_01_87_01_8A_11_B67_99_A0
h_F9_F6_BA_AA_96R_A89_E91~_8A_0C^K_B4)J1b9_0E_A6_03ECw|_08^_8A>_C3FK_B51_C3(_AA_F9_FD_028_D3_A3\5_EC_B7)_17)XU
r_B7=_BA_D2k_07_08_D5_F9r#0bA_E3+_B2_C6_83_BE_ABo/_B0_82_C5C;_18_8F_CEXL_B1_E2Ew_81l_89_1A5%_A7_9D_C8f_DC_96y_DA_9
0_DC_CE_03w_CD_89(e_EC0
_CA_96'6_C4;_93_C2_E8_E0P=_B9_AF_F5_E9_A5z_A8?H_B6_8D_9A_10_FFI_A0r_F4@=_C0_B8_C6/_E0_EC_C1_1F_E2_FD_E3_Fay_B3:~kK_
8C_1CmW?_BE7_EF_C9_1Dg_B8_C3A_A0_D32_A7T_C6_CE|_9F_C4_93_86_8B_CE_DF_F8_Jl_EE_D7_01_00_00
0

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:42:11 GMT
Content-Type: text/html
Last-Modified: Fri, 10 Apr 2026 18:57:21 GMT
Transfer-Encoding: chunked
Connection: keep-alive
ETag: W/"69d94811-a92"
Content-Encoding: gzip

4cd
_1F_8B_08_00_00_00_00_04_03_BDV_CDr_E44_10_BE_EFS4:PP_85_C7cg_92_C9_ B6_AB_B2_9B_DA_CAVm_AA_16_02_A9%_17J#+_B1@_
B6_8C\$;?_A7_BC_03_07_E0Dq_E4_C0_05_DE_80_BCl_9E_84_96d_CfX_86_9F_A580_E3_F1_A8_F5_D3_AD_FE_BA_Bf_96_9Ed_EF_95_8A_D9
_DB_96CekY<_C9_DC_1FH_DA|_E5_84_1B_E2:8~_8B'_00Y_CD~_05VQm_B8_CD|g/_A3C_02_F1f_A8_A15_CFI/_F8u_AB_B4%_C0Tcy_83S_AFE
|_AB_BC_E4_BD'<_F2_C2G
_1Aa_05_95_91aT_F2<_19_15Ya%|/>_E5N_03_877G_AF_E0_F1_FE|x_A9_BD_AA2_8B_C3_B8_DB_8D_14_CD_D7_A0_B9_CC_89_B1_B7_92_9B_
8As_B4Yi~9_F6_CC_981'o_16_07_1F_B2_95'o_FD~_9D_CC_B5k_A2_A6R_F4_C0\$5&~+M_9B_12_9Dv_FD8b_FA+p_FE<W79_99_C3_1C_D2_05>
_04_82C\$M_D1
_17W_15_FA_E8_DAT_0B_1AU_A2,y_93_13_AB;N_8A_AC_A5_B6_82K!q_9F_AC_D3_1A_F1x_A1_A4_D2_04_CA_9C_9C&Oa_EFd_9F_A6_90_A2n
_FCF_D8_EA_93_C5_A6_03_07_D2|_BB#J_CF_B7VD_E9E_1D~!Y_9C,_FB(_AD_F6|_94_F7_A3AJ_E6N_9C;_F1|Yy_89_C4E_16_A3c_1B|_DAL

_11_C7Q_D7_13_B0_89_11_1C_D7_0C_10:_C8_9CPS1N_A8_92_11_BB_96^_F1_C8_C7_E7_7F_04_10_F1_A1_C9_1C_F0_C1_97_FB_B9_E7(9 CF_E6I_82-_FF_E7_A1_85_04_A7^_D4_D8_B9_A8_A2_D4!_15_80A_E1_FC_00_DB_BB_B0_9CS)J_CA_C4_C3o_94_1C_8E_15_EBj_0C_9E2_03.U2
_D4_8E_FE_9Bn5x_7F_D6_AD8_D8_0E_F3_81U_A2Wp_0B_ADV_8C_1B_AAy_AD_0C_D0_CE_AA_FA_E1'+_18_12_06)_02!"_1D_95_AE_F9_8B [_0F_B1K>_CE_ACP_CD_A8_9EQ=_C9_CC*_ _8E_06_EDt_AD_1D_83_94_0E_ABq_FD\$ _AD_B5_BA^_C7_04G\$]_A1I4_889_E9x_F6e_ED_98_FE_C 2S_0E)E)_8B_FD_9C_E0" _E0g_AAM4mg#_D1_031_C3=_1En
N_F2#
0_B57z!_94_85I_87_AB6_C8_0F~c_C9dqP_01_AD_A4_8CWJ"=s_F2_05~_A2_D3SP0_B4_A2_E3c_14_1E_EF_BF_AF_A9_BES_90_CE_D3_83_C7 _FB_1F_86_E21h_80I_D5Y_8B_C0_B9}_ACI_139_F6_11_08V_C3_10J_AE_CE_E4_E4s_8C_89_F3_17(_B3_1D_95_A4x_FC_F1_D7_0E_936_9 Ee#_0B_82_85_CC_D4T_CA1_95h.)>_13_ED3_E8_0CE_E3_C5_B0W_D4S@K5_D6L_8F_C6_DA_A0_0C_B1_?_AA_1F_94_0FHx_9C_DD_C6K_AD_ DA:_85_00_8Fv6_1D_96_AEDSrW_92_08h_E5_FC_18_DD_F2_15_C8_87.'_17_AA_C1_D4p_F6_A9_D6_D4X_8D_AE_DE_82Q_D2bcH_CDI_F8_A6 _11_ _EF0_BC_D7_93a_8C_EE;_AA_E1_1E_9E_06c5t_ED_FFR_93_B4_ _9E_EC_F7_D1_F2d_AF_ _BE_A3_0C_E2_AC_8BSd_F9_C1I_91_ _E0p_B6 _9C/_87_F7r_96>_DD_83_F0v_B4_9F_ED_1F_1E_C8_85_9F_E0_DFQ_E2_97_F8_F7_EBd/h8O_0E_B0_16_FC_A9_0E_B8_90gk_8E#0_03_C7_8 F_06L_A7<_A7_DFt_0F_BFd_8E_C1c*_EE_AC_AD_B8Ii_A1_A0_A2w_18V_C1Bx_0C_97_9C1_A4:_D5_FF_B4_B8Q_16_E9_F6_12_CB_04_B5_EA _19_BC}}_F6_16>_C0:r3C_1E_BC_DF_ACL_FB_F1_E9_F3_0F_B74_EC&_EE_86_9F_C8
L_AD_C0_89_D0_A6_8C_F1_D6_E6dv#_CD_CD_10_BD!_93_CE6_1B\N8_F8=:_81_1D_D3_04_1ENS_A78_C2_12_D8_12_CF_C5_89_18_0E_C9N _99;r6_93\ _C9_C0_B3sr_10yC:_BCf_92S<H_B7_89=e_C0'_9D_D8_CA_F5_87_EFv_B9_FD_17_E4_1B_F6_8E_05_01#_E2.@c,w_CBJ_A8_E9x _C3_D8_DE@)_0CjI^_16o_86_9A_0Fx_C1
g_C7_BF_B0_EE_A8o'_B5_1D_EA_1Dv2_8A_81_E9_A3_14_FC_14=_92_BFUR_B8_D4_D8_8A_F6_BA_90hn:i_D7_DA_06q:_19q_0EG_8D_F35_8 B_C3_E1_EE_9A_97
SN_07_04B_D1+~_FF_19_FE_FEr_B6_AEKY<.uj_0C_D3_A2_B5'4_CB
m_DB_D9W_88*_DA_F4_BDx_BF_8C_C3_AD_0C_0F/_7F_01_FD_03_1F_E0q_19_92
_00_00
0

3 Content-Security-Policy HTTP Security Header Not Detected

port 8090/tcp

QID: 48001
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Content-Security-Policy](#)
Bugtraq ID: -
Service Modified: 03/11/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8090.
GET / HTTP/1.1
Host: 172.40.123.5:8090
Connection: Keep-Alive

QID: 48001
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: [Content-Security-Policy](#)
 Bugtraq ID: -
 Service Modified: 03/11/2019
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 9090.
 GET / HTTP/1.1
 Host: 172.40.123.5:9090
 Connection: Keep-Alive

QID: 48001
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: [Content-Security-Policy](#)
 Bugtraq ID: -
 Service Modified: 03/11/2019
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8002.
GET / HTTP/1.1
Host: 172.40.123.5:8002
Connection: Keep-Alive

 3 Content-Security-Policy HTTP Security Header Not Detected

port 8443/tcp

QID: 48001
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Content-Security-Policy](#)
Bugtraq ID: -
Service Modified: 03/11/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8443.
GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive

QID: 48001
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Content-Security-Policy](#)
Bugtraq ID: -
Service Modified: 03/11/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 9443.
GET / HTTP/1.1
Host: 172.40.123.5:9443
Connection: Keep-Alive

QID: 48001
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Content-Security-Policy](#)
Bugtraq ID: -
Service Modified: 03/11/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8089.
GET / HTTP/1.1
Host: 172.40.123.5:8089
Connection: Keep-Alive

 3 Content-Security-Policy HTTP Security Header Not Detected

port 5002/tcp

QID: 48001
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Content-Security-Policy](#)
Bugtraq ID: -
Service Modified: 03/11/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 5002.
GET / HTTP/1.1
Host: 172.40.123.5:5002
Connection: Keep-Alive

QID: 48001
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: [Content-Security-Policy](#)
 Bugtraq ID: -
 Service Modified: 03/11/2019
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8091.
 GET / HTTP/1.1
 Host: 172.40.123.5:8091
 Connection: Keep-Alive

QID: 82063
 Category: TCP/IP
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 05/29/2007
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 22, the host's uptime is 25 days, 14 hours, and 15 minutes. The TCP timestamps from the host are in units of 1 milliseconds.



2 Web Server HTTP Protocol Versions

port 80/tcp

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server Supports HTTP 2 on 80 port.Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1



2 Web Server HTTP Protocol Versions

port 443/tcp

QID: 45266
Category: Information gathering

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions

port 443/tcp over SSL

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server Supports HTTP 2 on 443 port.



2 Web Server HTTP Protocol Versions

port 8090/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8090 port.GET / HTTP/1.1



2 Web Server HTTP Protocol Versions

port 9090/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 9090 port.GET / HTTP/1.1



2 Web Server HTTP Protocol Versions

port 10250/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 10250 port.GET / HTTP/1.1



2 Web Server HTTP Protocol Versions

port 8002/tcp

QID:	45266
------	-------

Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8002 port.GET / HTTP/1.1



2 Web Server HTTP Protocol Versions

port 8443/tcp

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8443 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions

port 8086/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8086 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions

port 8000/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8000 port.GET / HTTP/1.1

2

Web Server HTTP Protocol Versions

port 10250/tcp over SSL

QID:

45266

Category:

Information gathering

Associated CVEs:

-

Vendor Reference:

-

Bugtraq ID:

-

Service Modified:

10/02/2024

User Modified:

-

Edited:

No

PCI Vuln:

No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server Supports HTTP 2 on 10250 port.

2

Web Server HTTP Protocol Versions

port 3000/tcp

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 3000 port.GET / HTTP/1.1



2 Web Server HTTP Protocol Versions

port 9443/tcp

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 9443 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions

port 8089/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8089 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions

port 8081/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8081 port.GET / HTTP/1.1

 2 Web Server HTTP Protocol Versions

port 9000/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 9000 port.GET / HTTP/1.1

 2 Web Server HTTP Protocol Versions

port 8095/tcp

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8095 port.GET / HTTP/1.1



2 Web Server HTTP Protocol Versions

port 8088/tcp

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8088 port.GET / HTTP/1.1

 2 Web Server HTTP Protocol Versions

port 5002/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5002 port.GET / HTTP/1.1

 2 Web Server HTTP Protocol Versions

port 8091/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8091 port.GET / HTTP/1.1

2

Web Server HTTP Protocol Versions

port 25000/tcp over SSL

QID:

45266

Category:

Information gathering

Associated CVEs:

-

Vendor Reference:

-

Bugtraq ID:

-

Service Modified:

10/02/2024

User Modified:

-

Edited:

No

PCI Vuln:

No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server Supports HTTP 2 on 25000 port.

2

Web Server HTTP Protocol Versions

port 25000/tcp

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 25000 port.GET / HTTP/1.1



2 Web Server HTTP Protocol Versions

port 8093/tcp

QID: 45266
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/02/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8093 port.GET / HTTP/1.1

 2 Web Server HTTP Protocol Versions

port 9091/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 9091 port.GET / HTTP/1.1

 1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.40.123.5	No registered hostname

1 Firewall Detected

QID: 34011
Category: Firewall
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 04/21/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 2869.

1 Traceroute

QID: 45006
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/09/2003
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	172.17.0.3	0.74ms	ICMP	
2	192.168.212.1	1.88ms	ICMP	
3	172.40.123.5	67.29ms	ICMP	

1 Host Scan Time - Scanner

QID: 45038
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/15/2022
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 11873 seconds

Start time: Fri, Apr 24 2026, 23:47:21 GMT

End time: Sat, Apr 25 2026, 03:05:14 GMT

1 Scan Activity per Port

QID: 45426
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/24/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	22	0:01:39
TCP	80	2:27:18
TCP	443	2:33:02

TCP	1720	0:16:19
TCP	3000	3:44:49
TCP	4118	0:00:56
TCP	5000	0:00:11
TCP	5002	3:01:36
TCP	5060	0:04:34
TCP	8000	4:06:04
TCP	8002	3:44:49
TCP	8081	2:37:28
TCP	8086	2:38:25
TCP	8088	2:43:48
TCP	8089	2:43:43
TCP	8090	3:50:50
TCP	8091	2:55:05
TCP	8093	2:37:36
TCP	8095	2:19:51
TCP	8443	2:36:09
TCP	9000	2:42:11
TCP	9090	4:06:06
TCP	9091	2:38:29
TCP	9443	2:48:39
TCP	10250	2:48:45
TCP	25000	2:49:01
UDP	68	0:00:07

1 SSH Algorithms ChaCha20-Poly1305 or CBC-EtM Detected

QID: 48259
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 02/12/2025
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The ChaCha20-Poly1305 algorithm and the CBC-EtM algorithm are known to be vulnerable to the SSH Prefix Truncation Vulnerability (Terrapin).

IMPACT:

The algorithms are known to be vulnerable to the SSH Prefix Truncation Vulnerability (Terrapin). Successful exploitation of the vulnerability may allow an attacker to downgrade the security of an SSH connection when using SSH extension negotiation. The impact in practice heavily depends on the supported extensions. Most commonly, this will impact the security of client authentication when using an RSA public key.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH Algorithms ChaCha20-Poly1305 or CBC-EtM detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False

1 Open UDP Services List

QID: 82004
Category: TCP/IP
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/11/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (<http://www.cert.org>).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
68	bootpc	Bootstrap Protocol Client	unknown

1 Open TCP Services List

QID: 82023
Category: TCP/IP
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -

Service Modified: 11/19/2025
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (<http://www.cert.org>).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www-http	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	
1720	netmeeting	h323hostcall h323hostcall	unknown	
3000	hbc	HBCI	http	
4118	unknown	unknown	unknown	
5000	Socket23	backdoor commplex-main	ssdp	
5002	rfe	radio free ethernet	http	
5060	sip	SIP	unknown	
8000	irdmi	iRDMI	http over ssl	
8002	unknown	unknown	http	
8081	unknown	unknown	http	
8086	unknown	unknown	http	
8088	unknown	unknown	http over ssl	
8089	unknown	unknown	http over ssl	
8090	unknown	unknown	http over ssl	
8091	unknown	unknown	http over ssl	
8093	unknown	unknown	http over ssl	
8095	unknown	unknown	http	
8443	unknown	unknown	http over ssl	
9000	cslistener	CSlistener	http	
9090	websm	WebSM vqserver administration port	http over ssl	
9091	unknown	unknown	http over ssl	
9443	unknown	unknown	http over ssl	

10250	unknown	unknown	http over ssl
25000	icl-twobase1	icl-twobase1	http over ssl

1 ICMP Replies Received

QID: 82040
 Category: TCP/IP
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 01/16/2003
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
 Timestamp Request (to trigger Timestamp Reply)
 Address Mask Request (to trigger Address Mask Reply)
 UDP Packet (to trigger Port Unreachable Reply)
 IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 2023	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 23929	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1047	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 9873	Port Unreachable
Time Exceeded (type=11 code=0)	(Various)	Time Exceeded
Unreachable (type=3 code=3)	UDP Port 456	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	23:47:24 GMT
Unreachable (type=3 code=3)	UDP Port 1701	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1037	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 13	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1053	Port Unreachable

1 Degree of Randomness of TCP Initial Sequence Numbers

QID: 82045
 Category: TCP/IP

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/19/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 987950223 with a standard deviation of 589102645. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5153 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID: 82046
Category: TCP/IP
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/27/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

N/A

Not Applicable

There is no exploitability information for this vulnerability.

There is no malware information for this vulnerability.

[illegible]

QID:	82056
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

Not Applicable

There is no exploitability information for this vulnerability.

There is no malware information for this vulnerability.

No results available

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

port 80/tcp

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Fri, 24 Apr 2026 23:50:32 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

 1 Default Web Page (Follow HTTP Redirection)

port 80/tcp

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Fri, 24 Apr 2026 23:51:01 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

 1 HTTP Response Method and Header Information Collected

port 80/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

GET / HTTP/1.1
Host: 172.40.123.5
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Fri, 24 Apr 2026 23:50:32 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive



1 Web Server Supports HTTP Request Pipelining

port 80/tcp

QID: 86565
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/22/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:80

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:80

HTTP/1.1 404 Not Found
Date: Sat, 25 Apr 2026 02:39:06 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

HTTP/1.1 404 Not Found
Date: Sat, 25 Apr 2026 02:39:06 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

 1 List of Web Directories

port 80/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/healthz/	brute force

 1 HTTP Response Method and Header Information Collected

port 443/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 443.

GET / HTTP/1.1
Host: 172.40.123.5
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Fri, 24 Apr 2026 23:56:31 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

1 HTTP Strict Transport Security (HSTS) Support Detected

port 443/tcp

QID: 86137
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2015
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubDomains



1 List of Web Directories

port 443/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/healthz/	brute force



1 SSH daemon information retrieving

port 22/tcp

QID: 38047
Category: General remote services
Associated CVEs: -

Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/20/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.
Supported ciphers suites reported in this qid are in server-preferred order.

For Red Hat ES 4:-

SSH1 supported	yes
Supported authentication methods for SSH1	RSA,password
Supported ciphers for SSH1	3des,blowfish
SSH2 supported	yes
Supported keys exchange algorithm for SSH2	diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported encryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported authentication methods for SSH2	publickey,gssapi-with-mic,password

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	sntrup761x25519-sha512@openssh.com, curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, ext-info-s, kex-strict-s-v00@openssh.com
Supported host key algorithms for SSH2	rsa-sha2-512, rsa-sha2-256, ecdsa-sha2-nistp256, ssh-ed25519
Supported decryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
Supported encryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
Supported decryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1

Supported encryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, password

1 SSH Banner

port 22/tcp

QID: 38050
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 10/30/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

IMPACT:

NA

SOLUTION:

NA

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.15

1 Default Web Page

port 443/tcp over SSL

QID: 12230
 Category: CGI
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/15/2019
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Fri, 24 Apr 2026 23:56:31 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection)

port 443/tcp over SSL

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Fri, 24 Apr 2026 23:58:56 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```



1 SSL Server Information Retrieval

port 443/tcp over SSL

QID: 38116
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH



1 SSL Session Caching Information

port 443/tcp over SSL

QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 443/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 443/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
TLSv1.3						
TLS13-AES-128-GCM-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe8192	8192	yes	202	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe8192	8192	yes	202	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe3072	3072	yes	132	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe4096	4096	yes	150	low

TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	x448	448	yes	224	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
TLS13-AES-256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	x448	448	yes	224	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x448	448	yes	224	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp384r1	384	yes	192	low



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 443/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no



1 TLS Secure Renegotiation Extension Support Information

port 443/tcp over SSL

QID: 42350
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tie renegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 443/tcp over SSL

QID: 48340
Category: Information gathering
Associated CVEs: -
Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
Bugtraq ID: -
Service Modified: 04/13/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 443/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	ac:34:3b:f4:c3:6c:fc:7e:49:cf:cb:65:4a:eb:0f:74
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
organizationName	Acme Co
commonName	Kubernetes Ingress Controller Fake Certificate
(0)SUBJECT NAME	
organizationName	Acme Co
commonName	Kubernetes Ingress Controller Fake Certificate
(0)Valid From	Apr 24 20:28:36 2026 GMT
(0)Valid Till	Apr 24 20:28:36 2027 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:ab:fd:51:61:39:53:29:14:af:94:91:50:f1:08:
(0)	83:bb:5e:43:6b:08:b1:76:5b:7c:a5:91:f3:c9:71:
(0)	2b:f0:86:cf:5e:d2:f0:fc:0f:89:46:fc:37:a8:e4:
(0)	e5:d2:08:66:c6:98:5f:bc:38:d1:e1:23:c9:8a:5a:
(0)	e7:99:15:be:a7:f3:9f:89:82:08:12:e2:8b:29:26:
(0)	c2:f2:47:0d:5c:b8:38:e5:85:9e:9f:13:bc:0e:42:
(0)	42:5e:65:21:c7:ee:4d:99:bd:58:fe:8e:f5:ea:ac:
(0)	7a:0b:0c:82:28:d1:5d:86:c7:2f:f4:22:8f:33:09:
(0)	41:99:6e:b4:5a:74:f6:f1:cd:0f:c7:01:e8:f9:99:
(0)	5c:7e:bf:86:99:39:b7:a6:eb:81:8a:40:5c:80:d0:
(0)	0f:57:14:05:ca:c2:97:5b:53:dd:7e:b7:a2:96:37:
(0)	02:1d:a0:2e:06:68:94:0a:6c:b5:10:55:74:a6:a4:
(0)	b1:33:81:df:1d:ac:b8:c1:a3:96:f5:07:67:95:36:
(0)	59:e1:e5:d8:e7:1c:5a:27:15:52:6a:c5:04:1d:61:
(0)	8b:98:1d:05:4c:aa:97:ac:99:1b:bf:a7:70:38:58:
(0)	41:c3:ef:d0:8d:cc:a6:6d:57:1e:c7:45:33:cb:dc:
(0)	9d:4c:9f:1c:f8:48:fa:4b:3b:3f:c7:b1:1a:eb:e8:
(0)	53:a7
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment

(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Alternative Name	DNS:ingress.local
(0)Signature	(256 octets)
(0)	22:94:4a:7f:aa:3e:89:3d:be:5e:10:cc:56:9c:46:26
(0)	6a:92:08:32:45:fa:01:e4:5e:fe:b1:55:59:8d:1b:0f
(0)	41:43:07:d9:c2:73:e7:5b:0c:a9:f0:50:c9:96:98:d1
(0)	1f:79:93:4a:fd:0f:d4:76:10:96:39:80:58:d1:15:0c
(0)	85:3d:b7:8d:13:39:ca:e4:8e:2d:3d:b0:84:27:af:a3
(0)	33:80:b0:11:e5:97:25:f6:50:a0:59:38:65:4f:14:df
(0)	4d:d9:66:f1:46:2c:b0:75:08:35:d8:64:42:eb:17:bd
(0)	13:2d:d0:37:f6:04:de:8d:77:8b:e8:4c:a5:bc:1f:10
(0)	57:bf:fa:08:de:10:c4:7b:4d:e1:db:20:b4:27:3a:6d
(0)	60:e3:55:0a:11:b6:63:29:db:bc:af:dc:7f:14:ff:65
(0)	fc:eb:c3:47:4b:23:b8:d0:c4:54:ee:a9:58:67:31:b1
(0)	3b:69:84:33:19:0a:f0:9d:0b:b2:15:5c:7c:3f:a8:7e
(0)	fa:d1:9a:e2:62:21:df:9c:bc:b0:5f:c1:1e:38:72:7a
(0)	c0:c9:b7:e0:a9:0e:29:6d:54:0b:e1:36:c0:74:8e:86
(0)	62:dc:d4:16:df:0f:ba:93:80:2e:26:3b:35:d6:0b:c4
(0)	99:36:0d:71:41:b9:46:53:7c:09:b9:50:3a:7c:ea:a6



1 Web Server Supports HTTP Request Pipelining

port 443/tcp over SSL

QID: 86565
 Category: Web server
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 02/22/2005
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:443

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:443

HTTP/1.1 404 Not Found
Date: Sat, 25 Apr 2026 02:39:08 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

HTTP/1.1 404 Not Found
Date: Sat, 25 Apr 2026 02:39:08 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```



1 Nginx Web Server Detected

port 8090/tcp

QID: 45433
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/15/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Nginx is a web server which can also be used as a reverse proxy, load balancer , mail proxy and HTTP cache.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Nginx Web Server Detected on 8090 over TCP.
Server: nginx/1.29.8

1 HTTP Public-Key-Pins Security Header Not Detected

port 8090/tcp

QID: 48002
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8090.
GET / HTTP/1.1
Host: 172.40.123.5:8090
Connection: Keep-Alive

1 HTTP Response Method and Header Information Collected

port 8090/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8090.

GET / HTTP/1.1
Host: 172.40.123.5:8090
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 00:19:04 GMT
Content-Type: text/html
Content-Length: 6718
Last-Modified: Mon, 13 Apr 2026 16:24:55 GMT
Connection: keep-alive
ETag: "69dd18d7-1a3e"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes



1 Referrer-Policy HTTP Security Header Not Detected

port 8090/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -

Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8090 port.
GET / HTTP/1.1
Host: 172.40.123.5:8090
Connection: Keep-Alive

1 List of Web Directories

port 8090/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/assets/	brute force
/#/	brute force
/assets/	web page
/#/	web page



1 Nginx Web Server Detected

port 9090/tcp

QID: 45433
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/15/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Nginx is a web server which can also be used as a reverse proxy, load balancer , mail proxy and HTTP cache.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Nginx Web Server Detected on 9090 over TCP.
Server: nginx/1.29.8



1 HTTP Public-Key-Pins Security Header Not Detected

port 9090/tcp

QID: 48002
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 9090.
GET / HTTP/1.1
Host: 172.40.123.5:9090
Connection: Keep-Alive



1 HTTP Response Method and Header Information Collected

port 9090/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 9090.

GET / HTTP/1.1
Host: 172.40.123.5:9090
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 01:03:29 GMT
Content-Type: text/html
Content-Length: 471
Last-Modified: Fri, 24 Apr 2026 20:28:05 GMT
Connection: keep-alive
ETag: "69ebd255-1d7"
Accept-Ranges: bytes

 1 Referrer-Policy HTTP Security Header Not Detected

port 9090/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 9090 port.
GET / HTTP/1.1
Host: 172.40.123.5:9090
Connection: Keep-Alive



1 List of Web Directories

port 9090/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/assets/	brute force
/assets/	web page



1 Apache Default Foreign Language File Still on Server

port 9090/tcp

QID: 86743
Category: Web server
Associated CVEs: -

Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/11/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Apache installs foreign language files along with index.html. The files are as follows:

index.html.ca
index.html.de
index.html.dk
index.html.ee

An attacker can get additional information about the Web server from these files.

IMPACT:

Sensitive system information may be disclosed, which can be utilized by an attacker to aid further attacks.

SOLUTION:

Apache recommends to remove these files from the Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /index.html.ru.iso-ru HTTP/1.1
Host: 172.40.123.5:9090
Connection: Keep-Alive

1 HTTP Response Method and Header Information Collected

port 10250/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 10250.

GET / HTTP/1.1
Host: 172.40.123.5:10250
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Sat, 25 Apr 2026 00:09:55 GMT
Content-Length: 19



1 List of Web Directories

port 10250/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/stats/	brute force



QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8002
Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8" />
  <link rel="icon" href="attu.svg" />
  <meta name="description" content="Attu, the best milvus management tool" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <meta name="theme-color" content="#000000" />
  <script src="/env-config.js"></script>
  <title>Attu</title>
  <script type="module" crossorigin src="/assets/index-CG2FxvRE.js"></script>
  <link rel="stylesheet" crossorigin href="/assets/index-psxnpbSW.css">
</head>

<body>
  <noscript>You need to enable JavaScript to run this app.</noscript>
  <div id="root"></div>
  <!--
    This HTML file is a template.
    If you open it directly in the browser, you will see an empty page.

    You can add webfonts, meta tags, or analytics to this file.
    The build step will place the bundled scripts into the <body> tag.

    To begin the development, run `npm start` or `yarn start`.
    To create a production bundle, use `npm run build` or `yarn build`.
  -->
</body>
```

</html>

1 Default Web Page (Follow HTTP Redirection)

port 8002/tcp

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8002
Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8" />
  <link rel="icon" href="attu.svg" />
  <meta name="description" content="Attu, the best milvus management tool" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <meta name="theme-color" content="#000000" />
  <script src="/env-config.js"></script>
  <title>Attu</title>
  <script type="module" crossorigin src="/assets/index-CG2FvxRE.js"></script>
  <link rel="stylesheet" crossorigin href="/assets/index-psxnpbSW.css">
</head>
```

```
<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root"></div>
<!--
```

This HTML file is a template.
If you open it directly in the browser, you will see an empty page.

You can add webfonts, meta tags, or analytics to this file.
The build step will place the bundled scripts into the <body> tag.

To begin the development, run `npm start` or `yarn start`.
To create a production bundle, use `npm run build` or `yarn build`.
-->
</body>
</html>

 1 HTTP Response Method and Header Information Collected

port 8002/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8002.

GET / HTTP/1.1
Host: 172.40.123.5:8002
Connection: Keep-Alive

HTTP/1.1 200 OK
Vary: Origin, Accept-Encoding
Access-Control-Allow-Credentials: true
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN

X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sat, 28 Feb 2026 03:26:25 GMT
ETag: W/"41c-19ca2487ae8"
Content-Type: text/html; charset=UTF-8
Content-Length: 1052
Date: Sat, 25 Apr 2026 00:13:54 GMT
Connection: keep-alive
Keep-Alive: timeout=5



1 HTTP Strict Transport Security (HSTS) Support Detected

port 8002/tcp

QID: 86137
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2015
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubDomains



1 Web Server Supports HTTP Request Pipelining

port 8002/tcp

QID: 86565
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/22/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:8002

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:8002

HTTP/1.1 200 OK
Vary: Origin, Accept-Encoding
Access-Control-Allow-Credentials: true
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sat, 28 Feb 2026 03:26:25 GMT
ETag: W/"41c-19ca2487ae8"
Content-Type: text/html; charset=UTF-8
Content-Length: 1052
Date: Sat, 25 Apr 2026 02:39:42 GMT
Connection: keep-alive
Keep-Alive: timeout=5

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8" />
  <link rel="icon" href="attu.svg" />
  <meta name="description" content="Attu, the best milvus management tool" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <meta name="theme-color" content="#000000" />
```

```

<script src="/env-config.js"></script>
<title>Attu</title>
<script type="module" crossorigin src="/assets/index-CG2FvxvRE.js"></script>
<link rel="stylesheet" crossorigin href="/assets/index-psxnpbSW.css">
</head>

<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root"></div>
<!--
  This HTML file is a template.
  If you open it directly in the browser, you will see an empty page.

  You can add webfonts, meta tags, or analytics to this file.
  The build step will place the bundled scripts into the <body> tag.

  To begin the development, run `npm start` or `yarn start`.
  To create a production bundle, use `npm run build` or `yarn build`.
-->
</body>

</html>
HTTP/1.1 404 Not Found
Vary: Origin, Accept-Encoding
Access-Control-Allow-Credentials: true
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
Content-Type: application/json; charset=utf-8
Content-Length: 99
ETag: W/"63-zVsAIDpNYtWej0hL4nL0KfKs2Og"
Date: Sat, 25 Apr 2026 02:39:42 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{"statusCode":404,"message":"ENOENT: no such file or directory, stat '/app/dist/build/index.html'"}

```



1 List of Web Directories

port 8002/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

[illegible]

1 Nginx Web Server Detected

port 8443/tcp

OID: 45433

Category: Information gathering

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/15/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Nginx is a web server which can also be used as a reverse proxy, load balancer , mail proxy and HTTP cache.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Nginx Web Server Detected on 8443 over TCP.
Server: nginx/1.25.4

1 HTTP Public-Key-Pins Security Header Not Detected

port 8443/tcp

QID: 48002
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8443.

GET / HTTP/1.1

Host: 172.40.123.5:8443

Connection: Keep-Alive



1 HTTP Response Method and Header Information Collected

port 8443/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8443.

GET / HTTP/1.1

Host: 172.40.123.5:8443

Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.25.4
Date: Sat, 25 Apr 2026 00:27:59 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT
Connection: keep-alive
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers:
Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

1 Referrer-Policy HTTP Security Header Not Detected

port 8443/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8443 port.
GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive



1 List of Web Directories

port 8443/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/#/	brute force



1 Default Web Page

port 8086/tcp

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8086
Connection: Keep-Alive

```
<html><head><meta http-equiv='refresh' content='1;url=/login?from=%2F'/><script id='redirect' data-redirect-url='/login?from=%2F'
src='/static/24c0402b/scripts/redirect.js'></script></head><body style='background-color:white; color:white;'>
Authentication required
<!--
-->

</body></html>
```

-CR-



1 Default Web Page (Follow HTTP Redirection)

port 8086/tcp

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1

```
<html><head><meta http-equiv='refresh' content='1;url=/login?from=%2F'/><script id='redirect' data-redirect-url='/login?from=%2F'  
src='/static/24c0402b/scripts/redirect.js'></script></head><body style='background-color:white; color:white;'>  
Authentication required  
<!--  
-->  
  
</body></html>
```

-CR-

 1 Jenkins Version Detected

port 8086/tcp

QID:	45284
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/08/2026
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Jenkins is an open source automation server written in Java.
Jenkins version has been found on the remote system.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

X-Jenkins: 2.541.3

 1 HTTP Response Method and Header Information Collected

port 8086/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8086.

GET / HTTP/1.1
Host: 172.40.123.5:8086
Connection: Keep-Alive

HTTP/1.1 403 Forbidden
Server: Jetty(12.1.5)
Date: Sat, 25 Apr 2026 00:37:17 GMT
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Reporting-Endpoints: content-security-policy:
http://172.40.123.5:8086/content-security-policy-reporting-endpoint/J9P16uqZxjPB-hlp4-O2D0TgsOID0dTcMyrhVli6m8=:YW5vbnltb3Vz::Lw==
Content-Security-Policy-Report-Only: base-uri 'none'; default-src 'self'; form-action 'self'; frame-ancestors 'self'; img-src 'self' data;;
script-src 'report-sample' 'self' usage.jenkins.io; style-src 'report-sample' 'self' 'unsafe-inline'; report-to content-security-policy;
report-uri http://172.40.123.5:8086/content-security-policy-reporting-endpoint/J9P16uqZxjPB-hlp4-O2D0TgsOID0dTcMyrhVli6m8=:YW5vbnltb3Vz::Lw==
Set-Cookie: JSESSIONID.9d431888=node01e1uj030idvoqqr37ixkd3yd3642.node0; Path=/; HttpOnly; SameSite=Lax
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
X-Hudson: 1.395
X-Jenkins: 2.541.3
X-Jenkins-Session: 24c0402b
Transfer-Encoding: chunked



1 Web Server Supports HTTP Request Pipelining

port 8086/tcp

QID: 86565
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/22/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:8086

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:8086

HTTP/1.1 403 Forbidden
Server: Jetty(12.1.5)
Date: Sat, 25 Apr 2026 02:40:26 GMT
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Reporting-Endpoints: content-security-policy:
<http://172.40.123.5:8086/content-security-policy-reporting-endpoint/J9P16uqZxjPB-hlp4-O2D0TgsOID0dTcMyrrhVli6m8=:YW5vbnltb3Vz::Lw==>
Content-Security-Policy-Report-Only: base-uri 'none'; default-src 'self'; form-action 'self'; frame-ancestors 'self'; img-src 'self' data:; script-src 'report-sample' 'self' usage.jenkins.io; style-src 'report-sample' 'self' 'unsafe-inline'; report-to content-security-policy; report-uri <http://172.40.123.5:8086/content-security-policy-reporting-endpoint/J9P16uqZxjPB-hlp4-O2D0TgsOID0dTcMyrrhVli6m8=:YW5vbnltb3Vz::Lw==>
Set-Cookie: JSESSIONID.9d431888=node01271bzd9yl3qcscsw1xi4f68f9268.node0; Path=/; HttpOnly; SameSite=Lax
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
X-Hudson: 1.395
X-Jenkins: 2.541.3
X-Jenkins-Session: 24c0402b
Transfer-Encoding: chunked

24D
<html><head><meta http-equiv='refresh' content='1;url=/login?from=%2F'/><script id='redirect' data-redirect-url='/login?from=%2F'
src='/static/24c0402b/scripts/redirect.js'></script></head><body style='background-color:white; color:white;'>
Authentication required
<!--
-->

</body></html>

0

HTTP/1.1 403 Forbidden
Server: Jetty(12.1.5)

Date: Sat, 25 Apr 2026 02:40:26 GMT
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Reporting-Endpoints: content-security-policy:
http://172.40.123.5:8086/content-security-policy-reporting-endpoint/6EIPNS9gzJcrD5sottPPTGqRCQTNrOKZHXdZb_kuM5k=:YW5vbnltb3Vz::L1FfRXZhc2l2ZS8=
Content-Security-Policy-Report-Only: base-uri 'none'; default-src 'self'; form-action 'self'; frame-ancestors 'self'; img-src 'self' data; script-src
'report-sample' 'self' usage.jenkins.io; style-src 'report-sample' 'self' 'unsafe-inline'; report-to content-security-policy; report-uri
http://172.40.123.5:8086/content-security-policy-reporting-endpoint/6EIPNS9gzJcrD5sottPPTGqRCQTNrOKZHXdZb_kuM5k=:YW5vbnltb3Vz::L1FfRXZhc2l2ZS8=
Set-Cookie: JSESSIONID.9d431888=node0ulyqfmc65jv11h6g99oph68x9269.node0; Path=/; HttpOnly; SameSite=Lax
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
X-Hudson: 1.395
X-Jenkins: 2.541.3
X-Jenkins-Session: 24c0402b
Transfer-Encoding: chunked

```
265
<html><head><meta http-equiv='refresh' content='1;url=/login?from=%2FQ_Evasive%2F'/><script id='redirect' data-redirect-url='/login?from=%2FQ_Evasive%2F'
src='/static/24c0402b/scripts/redirect.js'></script></head><body style='background-color:white; color:white;'>
Authentication required
<!--
-->

</body></html>

0
```

1 List of Web Directories		port 8086/tcp
QID:	86672	
Category:	Web server	
Associated CVEs:	-	
Vendor Reference:	-	
Bugtraq ID:	-	
Service Modified:	09/10/2004	
User Modified:	-	
Edited:	No	
PCI Vuln:	No	

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/logout/	brute force
/login	brute force
/static/	web page
/static/24c0402b/	web page
/static/24c0402b/scripts/	web page
/adjuncts/	web page
/adjuncts/24c0402b/	web page
/adjuncts/24c0402b/io/	web page
/adjuncts/24c0402b/io/jenkins/	web page

/adjuncts/24c0402b/io/jenkins/plugins/	web page
/adjuncts/24c0402b/io/jenkins/plugins/thememanager/	web page
/adjuncts/24c0402b/io/jenkins/plugins/thememanager/header/	web page
/static/24c0402b/jsbundles/	web page

1 Nginx Web Server Detected

port 8000/tcp

QID: 45433
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 10/15/2024
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

Nginx is a web server which can also be used as a reverse proxy, load balancer , mail proxy and HTTP cache.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Nginx Web Server Detected on 8000 over TCP.
 Server: nginx/1.29.8

1 HTTP Public-Key-Pins Security Header Not Detected

port 8000/tcp

QID: 48002
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 07/12/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8000.
GET / HTTP/1.1
Host: 172.40.123.5:8000
Connection: Keep-Alive



1 HTTP Response Method and Header Information Collected

port 8000/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8000.

GET / HTTP/1.1
Host: 172.40.123.5:8000
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 00:50:13 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 3142
Connection: keep-alive
Vary: Origin
Content-Security-Policy: frame-ancestors
Access-Control-Allow-Credentials: true
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 11 Aug 2025 12:14:01 GMT
ETag: W/"c46-198990d4728"
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type



1 Referrer-Policy HTTP Security Header Not Detected

port 8000/tcp

QID:	48131
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	01/18/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8000 port.

GET / HTTP/1.1

Host: 172.40.123.5:8000

Connection: Keep-Alive



1 List of Web Directories

port 8000/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/assets/	web page
/static/	brute force



1 Apache Default Foreign Language File Still on Server

port 8000/tcp

QID: 86743
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/11/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Apache installs foreign language files along with index.html. The files are as follows:

index.html.ca
index.html.de
index.html.dk
index.html.ee

An attacker can get additional information about the Web server from these files.

IMPACT:

Sensitive system information may be disclosed, which can be utilized by an attacker to aid further attacks.

SOLUTION:

Apache recommends to remove these files from the Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /index.html.ru.iso-ru HTTP/1.1
Host: 172.40.123.5:8000
Connection: Keep-Alive



1 Default Web Page

port 10250/tcp over SSL

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:10250
Connection: Keep-Alive

404 page not found

1 Default Web Page (Follow HTTP Redirection)

port 10250/tcp over SSL

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:10250
Connection: Keep-Alive

404 page not found

1 SSL Server Information Retrieval

port 10250/tcp over SSL

QID: 38116
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No

PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH



1 SSL Session Caching Information

port 10250/tcp over SSL

QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is disabled on the target.

**1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance**

port 10250/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	rejected
0399	rejected
0400	rejected
0499	rejected



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 10250/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
AES256-GCM-SHA384	RSA		2048	no	110	low
AES128-GCM-SHA256	RSA		2048	no	110	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low

ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 10250/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Heartbeat	no
Cipher priority controlled by	client and server
OCSP stapling	no

SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no



1 TLS Secure Renegotiation Extension Support Information

port 10250/tcp over SSL

QID: 42350
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/21/2016
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tie renegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 10250/tcp over SSL

QID: 48340
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
 Bugtraq ID: -
 Service Modified: 04/13/2026

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 10250/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	32:0a:a3:a1:92:00:ef:fb:65:a1:31:61:fb:16:87:ce:8d:19:88:d7
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
commonName	10.152.183.1
(0)SUBJECT NAME	
commonName	system:node:anqialazmv01
organizationName	system:nodes
(0)Valid From	Aug 15 16:30:18 2025 GMT
(0)Valid Till	Aug 13 16:30:18 2035 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c1:4c:36:4e:ce:bc:8f:5e:68:82:a6:ee:d7:9a:
(0)	12:db:75:39:42:8f:ce:3c:ce:eb:a3:69:b9:57:44:
(0)	ac:f7:7c:9e:93:07:47:5e:21:d7:18:31:a5:1a:36:
(0)	76:8f:4d:b2:09:ad:c2:9c:c0:73:ea:7e:99:68:22:
(0)	91:d4:2d:8c:2e:3a:73:f8:7e:90:2b:f6:5b:0c:b1:
(0)	9f:1a:e9:1a:c4:78:50:92:0e:0e:4c:9e:be:fc:df:
(0)	6d:e0:69:1d:e0:46:8e:4a:3a:91:fb:eb:f0:e9:1c:
(0)	f2:d3:87:d1:48:16:c4:b5:c1:67:9d:cd:73:e6:07:
(0)	16:bc:83:de:57:ef:d1:61:68:f6:ec:e7:77:2c:fa:
(0)	a4:ae:f1:58:10:4d:2a:0d:b6:f6:e6:51:d7:be:12:
(0)	fa:0c:aa:36:1b:a5:34:2e:72:62:6c:45:8b:ca:b7:
(0)	41:79:3f:77:de:41:f1:cb:78:9e:81:85:79:c9:bd:
(0)	13:8a:26:e3:3a:9f:9c:c0:a1:49:19:13:5d:94:e5:
(0)	58:ef:27:98:26:ef:94:d8:4c:e3:32:39:87:c9:6d:
(0)	68:39:54:77:da:f1:d3:87:73:f5:b7:46:0e:d9:69:
(0)	99:5c:22:e8:30:60:95:b0:af:74:3c:c3:5a:9d:aa:
(0)	71:d2:c7:dc:43:9d:ae:d4:d9:7c:c1:ee:6d:f0:77:
(0)	b2:0d
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Subject Alternative Name	DNS:anqialazmv01, IP Address:172.40.123.5, IP Address:172.18.0.1
(0)Signature	(256 octets)
(0)	32:0e:7a:60:c9:e1:af:f9:e5:b6:78:d9:f7:49:12:7f
(0)	95:1a:fa:14:b3:e8:ad:2a:ca:a1:00:b2:04:3e:46:ad
(0)	6f:74:28:8b:54:71:46:c9:14:9c:3f:c8:81:56:d3:37
(0)	6a:01:55:7f:6d:6d:d4:0e:16:59:9c:67:32:96:de:db
(0)	d3:18:c0:9c:6f:02:a2:43:db:4f:f8:5c:81:a1:bb:60
(0)	19:ad:b3:c2:53:0e:db:43:ba:c4:8f:07:1d:6a:b5:6f
(0)	4d:70:4a:b0:14:2a:66:65:bc:95:3a:43:7c:cd:d7:a5
(0)	84:a2:96:58:ba:85:42:35:5e:43:fa:20:f1:a9:d5:b0
(0)	48:4b:51:ae:03:1a:d8:a1:0f:d4:f6:bd:46:f8:d6:90
(0)	46:33:32:7c:a2:f8:b3:61:97:c4:4c:20:be:68:a2:3a
(0)	54:97:8a:de:ce:6f:0c:fc:a2:5a:7f:b3:0b:e7:a7:91
(0)	de:96:70:ed:a9:60:0b:d6:8e:72:37:7b:97:98:68:b2
(0)	8e:93:f7:2a:fa:c8:d7:1c:5f:22:82:8b:b0:9e:be:00
(0)	d4:d7:bf:16:1d:d4:4c:81:8a:49:58:fc:7e:a0:66:60

(0)	87:e1:b0:38:14:3d:38:be:60:7c:55:11:41:5f:55:c8
(0)	03:ba:5c:6b:03:04:35:d8:ed:13:bd:77:50:0d:4c:98

1 Web Server Supports HTTP Request Pipelining

port 10250/tcp over SSL

QID: 86565
 Category: Web server
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 02/22/2005
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
 Host:172.40.123.5:10250

GET /Q_Evasive/ HTTP/1.1
 Host:172.40.123.5:10250

HTTP/1.1 404 Not Found
 Content-Type: text/plain; charset=utf-8
 X-Content-Type-Options: nosniff
 Date: Sat, 25 Apr 2026 02:39:20 GMT
 Content-Length: 19

404 page not found
 HTTP/1.1 404 Not Found
 Content-Type: text/plain; charset=utf-8
 X-Content-Type-Options: nosniff
 Date: Sat, 25 Apr 2026 02:39:20 GMT
 Content-Length: 19

404 page not found

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8090
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 00:19:04 GMT
Content-Type: text/html
Content-Length: 6718
Last-Modified: Mon, 13 Apr 2026 16:24:55 GMT
Connection: keep-alive
ETag: "69dd18d7-1a3e"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

<!DOCTYPE html>
<html lang="es">

<head>
<meta charset="UTF-8">
<title>Chat Eureka</title>
<link href="https://fonts.googleapis.com/css2?family=Nunito+Sans:wght@400;600;700;800&display=swap" rel="stylesheet">
<link rel="stylesheet" href="style.css">

</head>

<body>

<!-- Overlay de Trminos y Condiciones (sin cambios) -->

<div id="terms_overlay" class="terms-overlay" role="dialog" aria-modal="true" aria-labelledby="terms_title">

<div class="terms-card">

<h2 id="terms_title">Trminos y Condiciones</h2>

<div class="terms-content" id="terms_content">

<pre>

Trminos y Condiciones de Uso y Aviso de Privacidad del Chatbot Eureka 2.0 ANLA
Bienvenido al chatbot informativo de Eureka 2.0 ANLA

Antes de utilizar este servicio, es fundamental que lea, comprenda y acepte los siguientes trminos y condiciones que regulan su uso. El acceso y utilizacin de este chatbot implica la aceptacin expresa de las clusulas que se detallan a continuacin.

1. Naturaleza y Alcance del Servicio

Carcter meramente informativo: Las respuestas que ofrece este chatbot tienen un propsito exclusivamente orientativo. Se sustentan en documentacin pblica y oficial disponible, pero no deben considerarse completas ni definitivas.

Uso de inteligencia artificial: Este chatbot funciona mediante modelos de inteligencia artificial que procesan la informacin suministrada por el usuario. Por ello, las respuestas pueden contener imprecisiones o interpretaciones aproximadas y deben ser verificadas antes de adoptar decisiones.

No constituye asesora legal ni tcnica: La informacin aqu proporcionada no reemplaza el anlisis, la interpretacin ni la asesora de profesionales cualificados. En ningn caso podr entenderse como una opinin vinculante de la ANLA. Para consultas con validez jurdica o tcnica, se recomienda acudir a un experto y/o a los canales oficiales de la Entidad.

Herramienta complementaria: Este chatbot es un canal de apoyo informativo y no sustituye los mecanismos formales de atencin al ciudadano. No tiene capacidad para tramitar solicitudes, responder PQRS (Petitionen, Quejas, Reclamos, Sugerencias y Denuncias) ni gestionar radicaciones. Para estos fines deber acudir exclusivamente a los canales oficiales de la ANLA.

2. Limitaciones del Contenido

El sistema est programado para no procesar ni responder a consultas relacionadas con:

Informacin sobre expedientes, licencias, permisos o trmites especficos en curso.

Datos personales o sensibles del usuario o de terceros.

Programacin o detalles logsticos de audiencias pblicas, reuniones o eventos.

Opiniones, valoraciones subjetivas o juicios de valor.

3. Validacin y Seguridad de la Informacin

Contraste con fuentes oficiales: Por motivos de seguridad y confiabilidad, se recomienda verificar toda la informacin proporcionada en este chatbot directamente en la plataforma oficial Eureka 2.0 u otros canales oficiales de la ANLA.

Limitaciones propias de la IA: Debido al estado actual de la tecnologa, el chatbot puede, en casos aislados, generar errores u ofrecer informacin imprecisa (alucinaciones). Por esta razn, se insiste en la necesidad de validar siempre los datos en las fuentes oficiales.

4. Poltica de Privacidad y Mejora Continua

La interaccin con el chatbot podr ser utilizada con fines de anlisis estadstico y mejora del servicio.

Esta informacin se recopila de manera anntima, sin almacenar datos personales identificables (como nombres, nmeros de identificacin o correos electrnicos).

La retroalimentacin de los usuarios es esencial para optimizar la calidad de la herramienta, siempre dentro de parmetros de seguridad y confidencialidad.

5. Exclusin de Responsabilidad

La ANLA no asume responsabilidad alguna por:

Las decisiones adoptadas por los usuarios con base en la informacin suministrada por el chatbot.

Cualquier error, inconsistencia o falta de actualizacin de la informacin generada por el sistema.

El uso indebido del chatbot o la interpretacin errnea de las respuestas.

6. Aceptacin de los Trminos

El inicio de la conversacin con el chatbot constituye prueba de que el usuario ha leído, comprendido y aceptado estos Trminos y Condiciones.

Si no est de acuerdo con ellos, le solicitamos abstenerse de utilizar este servicio.

</pre>

</div>

<div class="terms-actions">

<button id="accept_btn" class="btn primary">Acepto</button>

<button id="decline_btn" class="btn danger">No acepto</button>

</div>

</div>

<div id="chat_app">

<main>

<header class="anla-header">

</header>

<h1>Chat Eureka</h1>

<div class="chat-container">

<div id="chat_response">

```

        <div class="welcome-message">Hola! Soy Eureka, tu asistente virtual. En qu puedo ayudarte hoy?</div>
    </div>

</main>

<form onsubmit="sendMessage(event)">
<input type="text" id="messageText" placeholder="Escribe tu pregunta" aria-label="Tu pregunta para Eureka" />
<button type="submit">Enviar</button>
<!-- Botn TTS -->
<button type="button" id="speak_btn" class="speak-btn" aria-label="Escuchar respuesta" title="Escuchar respuesta">
    Escuchar
</button>
</form>

<footer class="site-footer" aria-hidden="true">
    Copyrigh 2020 Herramienta de consulta EUREKA!!
    Todos los derechos reservados Gobierno de Colombia - ANLA
</footer>

</div> <!-- /#chat_app -->

<!-- NUEVO: mensaje cuando el usuario NO acepta -->
<div id="blocked" class="blocked" hidden aria-live="polite">
<div class="blocked-card">
    <h2>Acceso no permitido</h2>
    <p>No se puede acceder al chatbot si no se aceptan los Trminos y Condiciones.</p>
</div>
</div>

<script src="script.js"></script>
</body>

</html>

```



1 Default Web Page (Follow HTTP Redirection)

port 8090/tcp over SSL

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8090
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 00:21:10 GMT
Content-Type: text/html
Content-Length: 6718
Last-Modified: Mon, 13 Apr 2026 16:24:55 GMT
Connection: keep-alive
ETag: "69dd18d7-1a3e"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

```
<!DOCTYPE html>  
<html lang="es">
```

```
<head>  
  <meta charset="UTF-8">  
  <title>Chat Eureka</title>  
  <link href="https://fonts.googleapis.com/css2?family=Nunito+Sans:wght@400;600;700;800&display=swap"  
    rel="stylesheet">  
  <link rel="stylesheet" href="style.css">  
</head>
```

```
<body>
```

```
  <!-- Overlay de Trminos y Condiciones (sin cambios) -->  
  <div id="terms_overlay" class="terms-overlay" role="dialog" aria-modal="true" aria-labelledby="terms_title">  
    <div class="terms-card">  
      <h2 id="terms_title">Trminos y Condiciones</h2>  
      <div class="terms-content" id="terms_content">  
        <pre>  
          Trminos y Condiciones de Uso y Aviso de Privacidad del Chatbot Eureka 2.0 ANLA  
          Bienvenido al chatbot informativo de Eureka 2.0 ANLA
```

Antes de utilizar este servicio, es fundamental que lea, comprenda y acepte los siguientes trminos y condiciones que regulan su uso. El acceso y utilizacin de este chatbot implica la aceptacin expresa de las clusulas que se detallan a continuacin.

1. Naturaleza y Alcance del Servicio

Carcter meramente informativo: Las respuestas que ofrece este chatbot tienen un propsito exclusivamente orientativo. Se sustentan en documentacin pblica y oficial disponible, pero no deben considerarse completas ni definitivas.

Uso de inteligencia artificial: Este chatbot funciona mediante modelos de inteligencia artificial que procesan la informacin suministrada por el usuario. Por ello, las respuestas pueden contener imprecisiones o interpretaciones aproximadas y deben ser verificadas antes de adoptar decisiones.

No constituye asesora legal ni tcnica: La informacin aqu proporcionada no reemplaza el anlisis, la interpretacin ni la asesora de profesionales cualificados. En ningn caso podr entenderse como una opinin vinculante de la ANLA. Para consultas con validez jurdica o tcnica, se recomienda acudir a un experto y/o a los canales oficiales de la Entidad.

Herramienta complementaria: Este chatbot es un canal de apoyo informativo y no sustituye los mecanismos formales de atencin al ciudadano. No tiene capacidad para tramitar solicitudes, responder PQRS (Petitionen, Quejas, Reclamos, Sugerencias y Denuncias) ni gestionar radicaciones. Para estos fines deber acudir exclusivamente a los canales oficiales de la ANLA.

2. Limitaciones del Contenido

El sistema est programado para no procesar ni responder a consultas relacionadas con:

Informacin sobre expedientes, licencias, permisos o trmites especficos en curso.

Datos personales o sensibles del usuario o de terceros.

Programacin o detalles logsticos de audiencias pblicas, reuniones o eventos.

Opiniones, valoraciones subjetivas o juicios de valor.

3. Validacin y Seguridad de la Informacin

Contraste con fuentes oficiales: Por motivos de seguridad y confiabilidad, se recomienda verificar toda la informacin proporcionada en este chatbot directamente en la plataforma oficial Eureka 2.0 u otros canales oficiales de la ANLA.

Limitaciones propias de la IA: Debido al estado actual de la tecnologa, el chatbot puede, en casos aislados, generar errores u ofrecer informacin imprecisa (alucinaciones). Por esta razn, se insiste en la necesidad de validar siempre los datos en las fuentes oficiales.

4. Poltica de Privacidad y Mejora Continua

La interaccin con el chatbot podr ser utilizada con fines de anlisis estadstico y mejora del servicio.

Esta informacin se recopila de manera anónima, sin almacenar datos personales identificables (como nombres, nmeros de identificacin o correos

electronicos).

La retroalimentación de los usuarios es esencial para optimizar la calidad de la herramienta, siempre dentro de parámetros de seguridad y confidencialidad.

5. Exclusion de Responsabilidad

La ANLA no asume responsabilidad alguna por:

Las decisiones adoptadas por los usuarios con base en la información suministrada por el chatbot.

Cualquier error, inconsistencia o falta de actualización de la información generada por el sistema.

El uso indebido del chatbot o la interpretación errónea de las respuestas.

6. Aceptación de los Términos

El inicio de la conversación con el chatbot constituye prueba de que el usuario ha leído, comprendido y aceptado estos Términos y Condiciones.

Si no estás de acuerdo con ellos, le solicitamos abstenerse de utilizar este servicio.

```
</pre>
</div>
<div class="terms-actions">
  <button id="accept_btn" class="btn primary">Acepto</button>
  <button id="decline_btn" class="btn danger">No acepto</button>
</div>
</div>
</div>

<div id="chat_app">

  <main>

    <header class="anla-header">
      
      <a href="https://www.anla.gov.co/07rediseureka2024" target="_blank">
        
      </a>
    </header>

    <h1>Chat Eureka</h1>

    <div class="chat-container">
      <div id="chat_response">
        <div class="welcome-message">Hola! Soy Eureka, tu asistente virtual. En qué puedo ayudarte hoy?</div>
      </div>
    </div>

  </main>

  <form onsubmit="sendMessage(event)">
    <input type="text" id="messageText" placeholder="Escribe tu pregunta" aria-label="Tu pregunta para Eureka" />
    <button type="submit">Enviar</button>
    <!-- Botón TTS -->
    <button type="button" id="speak_btn" class="speak-btn" aria-label="Escuchar respuesta" title="Escuchar respuesta">
      Escuchar
    </button>
  </form>

  <footer class="site-footer" aria-hidden="true">
    Copyright 2020 Herramienta de consulta EUREKA!!
    Todos los derechos reservados Gobierno de Colombia - ANLA
  </footer>

</div> <!-- /#chat_app -->

<!-- NUEVO: mensaje cuando el usuario NO acepta -->
<div id="blocked" class="blocked" hidden aria-live="polite">
  <div class="blocked-card">
    <h2>Acceso no permitido</h2>
    <p>No se puede acceder al chatbot si no se aceptan los Términos y Condiciones.</p>
  </div>
</div>

<script src="script.js"></script>
</body>

</html>
```



1 SSL Server Information Retrieval

port 8090/tcp over SSL

QID: 38116

Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 05/24/2016
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
CAMELLIA128-SHA256	RSA	RSA	SHA256	Camellia(128)	MEDIUM
CAMELLIA256-SHA256	RSA	RSA	SHA256	Camellia(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ARIA128-GCM-SHA256	RSA	RSA	AEAD	ARIAGCM(128)	MEDIUM

ARIA256-GCM-SHA384	RSA	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-ARIA128-GCM-SHA256	ECDH	RSA	AEAD	ARIAGCM(128)	MEDIUM
ECDHE-RSA-ARIA256-GCM-SHA384	ECDH	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-CAMELLIA128-SHA256	ECDH	RSA	SHA256	Camellia(128)	MEDIUM
ECDHE-RSA-CAMELLIA256-SHA384	ECDH	RSA	SHA384	Camellia(256)	HIGH
AES128-CCM	RSA	RSA	AEAD	AESCCM(128)	MEDIUM
AES256-CCM	RSA	RSA	AEAD	AESCCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					



1 SSL Session Caching Information

port 8090/tcp over SSL

QID: 38291
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/19/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 8090/tcp over SSL

QID: 38597
 Category: General remote services

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 8090/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
AES256-SHA256	RSA		2048	no	110	low
AES128-SHA256	RSA		2048	no	110	low
AES256-CCM	RSA		2048	no	110	low
AES128-CCM	RSA		2048	no	110	low
ARIA256-GCM-SHA384	RSA		2048	no	110	low
ARIA128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA256	RSA		2048	no	110	low
AES256-GCM-SHA384	RSA		2048	no	110	low
AES128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA	RSA		2048	no	110	low
CAMELLIA128-SHA	RSA		2048	no	110	low
AES256-SHA	RSA		2048	no	110	low
AES128-SHA	RSA		2048	no	110	low
CAMELLIA128-SHA256	RSA		2048	no	110	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA384	ECDHE	x448	448	yes	224	low

ECDHE-RSA-AES256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 8090/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no



1 Secure Sockets Layer (SSL) Certificate Transparency Information

port 8090/tcp over SSL

QID: 38718
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.anla.gov.co, O=U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA, ST=Distrito Capital de Bogot, C=CO			
Certificate	no	(unknown)	(unknown)	d809553b944f7affc816196f9 44f85abb0f8fc5e8755260f15 d12e72bb454b14	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	af67883b57b04edd8fa6d97ef 62ea8eb810ac77160f0245e55 d60c2fe785873a	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	acab30706cebec8431f413d2f 4915f111e422443b1f2a68c4f 3c2b3ba71e02c3	Thu 01 Jan 1970 12:00:00 AM GMT



1 Reports if server supports Post Quantum Cryptographic(PQC) Key Exchange Algorithm

port 8090/tcp over SSL

QID: 38994
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

It reports complete list of all host-supported PQC key-exchange algorithms along with full handshake details.
If server hosts any service

over TLS1.3, then a probe is sent to validate if the service supports following PQC key exchange

algorithms.
MLKEM512
MLKEM768
MLKEM1024
X25519MLKEM768
SecP256r1MLKEM768
SecP384r1MLKEM1024

Field
Description

Cipher name
Cipher used

Protocol
TLS
version

Key-exchange
Negotiated PQC KEX

Authentication
Signature algorithm

MAC
Message authentication code

Encryption + key
strength
Encryption mode and key size

NIST security strength
Security strength (NIST
equivalent)

Reference: <https://csrc.nist.gov/groups/ST/post-quantum-crypto/evaluation-criteria.html>

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	STRENGTH
TLS13-AES-256-GCM-SHA384	X25519MLKEM768	RSA-PSS	AEAD	AESGCM(256)	192-bit



1 Reports Signature Algorithm used in Post Quantum Cryptographic(PQC) detection using QID 38994

port 8090/tcp over SSL

QID: 38995
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

If server hosts any service over TLS1.3, then a probe is sent to validate if the service supports PQC key exchange algorithms as part of QID38994.

This QID reports Signature Algorithm used by the service for Post Quantum Cryptographic(PQC) SSL handshake using QID 38994.

It

reports server's preferred PQC signature algorithm.

This QID is planned for future deprecation.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Preferred PQC Signature Algorithm: RSA-PSS

**1 TLS Secure Renegotiation Extension Support Information**

port 8090/tcp over SSL

QID:	42350
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tier negotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2) port 8090/tcp over SSL

QID:48340

Category:Information gathering

Associated CVEs:-

Vendor Reference:[SSL/TLS Server supports TLSv1.2](#)

Bugtraq ID:-

Service Modified:04/13/2026

User Modified:-

Edited:No

PCI Vuln:No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported

1 SSL Certificate - Information port 8090/tcp over SSL

QID:86002

Category:Web server

Associated CVEs:-

Vendor Reference:-

Bugtraq ID:-

Service Modified:03/07/2020

User Modified:-

Edited:No

PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	b2:f8:3d:72:1f:f3:a7:29:60:a2:df:c3:eb:8c:4e:fe
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(0)SUBJECT NAME	
countryName	CO
stateOrProvinceName	Distrito Capital de Bogotá\C3\A1
organizationName	U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA
commonName	*.anla.gov.co
(0)Valid From	Oct 22 00:00:00 2025 GMT
(0)Valid Till	Nov 3 23:59:59 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c5:22:80:6e:68:2e:0a:69:6c:67:0c:b8:ee:74:
(0)	e6:56:64:4b:b8:7c:61:47:27:e3:6d:60:a6:34:1e:
(0)	77:20:80:97:2e:ef:ac:2a:8c:52:08:59:9b:33:1e:
(0)	46:70:61:83:8e:1a:85:af:55:76:33:a3:94:c1:04:
(0)	e3:2c:f3:01:07:35:c1:4a:dc:48:47:42:2f:ae:f1:
(0)	fd:b7:49:e5:ff:21:ba:47:cb:bf:1e:4d:13:d3:32:
(0)	17:73:33:65:22:03:ee:2d:36:f2:bc:5a:a5:7d:ad:
(0)	03:01:c2:c0:fe:95:9e:af:81:95:bb:43:59:95:4a:
(0)	bf:82:31:de:e6:1b:43:f4:11:c0:36:be:2c:00:fc:
(0)	2f:97:4b:bb:78:87:61:6e:29:1a:91:8b:a6:2d:f6:
(0)	27:75:93:c2:46:8d:84:cf:b6:8a:69:98:4d:2d:b3:
(0)	4c:1d:44:ea:f6:a4:f9:00:5b:c8:8a:ed:77:66:b3:

(0)	ce:b1:87:b7:e7:52:95:da:e2:08:0d:bb:03:78:02:
(0)	17:46:ce:46:e7:83:f1:1d:ba:47:a3:e2:0e:e3:7b:
(0)	dc:ff:47:79:09:ff:a4:5a:2d:58:4c:d4:1c:24:af:
(0)	a1:aa:ed:50:96:8e:9c:e5:7a:a2:ba:91:53:30:4c:
(0)	42:04:c6:39:7b:c1:f3:88:68:7b:6f:5a:8b:1d:ef:
(0)	5c:5f
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(0)X509v3 Subject Key Identifier	3A:B2:87:43:6F:E2:96:F3:ED:40:44:B2:5F:8C:7E:8B:8F:2C:CD:44
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.1.3.4
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.2
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI: http://crl.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crl
(0)Authority Information Access	CA Issuers - URI: http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
(0)	OCSP - URI: http://ocsp.sectigo.com
(0)X509v3 Subject Alternative Name	DNS:*.anla.gov.co, DNS:anla.gov.co
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:
(0)	B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14
(0)	Timestamp : Oct 22 21:05:01.112 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:DB:DF:24:6B:4B:B4:A3:AF:88:F0:38:
(0)	D1:3F:21:84:EF:C7:FF:E9:37:FB:FE:CD:B6:CA:04:EF:
(0)	45:22:C8:5B:32:02:21:00:F3:94:94:8C:3F:DA:C9:34:
(0)	51:AE:9A:73:07:1B:37:36:DC:28:62:98:D7:5C:66:52:
(0)	98:71:17:EA:46:23:10:97
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AF:67:88:3B:57:B0:4E:DD:8F:A6:D9:7E:F6:2E:A8:EB:
(0)	81:0A:C7:71:60:F0:24:5E:55:D6:0C:2F:E7:85:87:3A
(0)	Timestamp : Oct 22 21:05:01.223 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:D2:A5:92:31:F6:F8:92:C8:0D:45:20:
(0)	A9:43:B4:3D:09:ED:63:29:FE:6C:BF:13:91:72:85:72:
(0)	ED:AF:05:9C:32:02:20:08:8A:F2:6D:EA:45:68:1A:22:
(0)	08:F4:76:CA:54:F5:B5:75:78:5E:A5:3B:2B:94:42:20:
(0)	03:D1:89:A3:78:FC:78
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AC:AB:30:70:6C:EB:EC:84:31:F4:13:D2:F4:91:5F:11:
(0)	1E:42:24:43:B1:F2:A6:8C:4F:3C:2B:3B:A7:1E:02:C3
(0)	Timestamp : Oct 22 21:05:00.999 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256

(0)	30:45:02:20:7A:D5:12:14:07:82:C9:A8:23:A7:95:43:
(0)	83:2B:93:B8:98:74:39:EA:8B:81:EE:6B:D9:1C:CB:DB:
(0)	50:74:D2:BA:02:21:00:C0:5F:F6:05:5B:47:AB:76:2E:
(0)	57:C7:FB:81:9B:91:F0:94:D6:15:89:F5:92:BF:31:F6:
(0)	02:CB:61:FB:61:95:9F
(0)Signature	(384 octets)
(0)	6f:c0:09:87:ec:ea:a5:4c:65:e0:96:7f:ee:cd:75:35
(0)	51:57:14:d5:af:5b:ed:55:e5:c4:27:67:93:7e:af:0a
(0)	ad:d2:a5:b9:86:c9:52:60:fc:8e:01:3c:33:bc:68:e2
(0)	7e:29:00:f6:4b:55:d6:1b:1e:a5:3e:e7:65:02:a5:c5
(0)	9d:6a:a2:d2:7e:68:e5:19:af:6d:81:db:29:c8:c8:6b
(0)	20:fa:eb:0b:70:20:be:bc:bb:89:48:ae:d4:d1:a8:ae
(0)	5c:01:be:87:43:5a:c6:43:b6:4a:de:24:a3:02:3b:67
(0)	d4:03:ab:90:d1:68:e0:7f:c7:f5:7d:15:2c:c7:bd:bd
(0)	35:33:ba:a3:1f:c6:a9:57:aa:a6:c7:ad:98:be:2a:8f
(0)	cb:c2:2e:1e:7f:7c:0f:e4:f0:a0:61:5a:24:66:24:ae
(0)	19:1c:8b:9f:3a:bc:a1:b4:47:71:63:43:2c:01:59:7c
(0)	9a:6a:88:aa:5f:f4:91:4a:7f:28:08:7b:61:52:4b:da
(0)	20:a9:e7:0e:35:a9:87:c5:1c:74:86:d2:56:7a:87:eb
(0)	03:73:4c:44:6e:c8:fd:b0:d0:f6:1f:d0:69:82:ab:57
(0)	d4:6d:2c:d7:7b:5a:60:ce:20:2a:6a:1f:0f:43:2a:79
(0)	f0:74:86:d8:6c:dc:86:a5:ca:98:d8:ae:38:79:36:38
(0)	2d:a1:02:36:5d:c2:04:3f:1a:f5:ea:00:99:b7:78:0c
(0)	fe:36:07:9b:5d:21:f9:14:65:37:d8:d8:e5:fd:ee:1a
(0)	c0:c3:a8:d7:0d:d5:a8:d2:0b:da:c5:c8:39:03:52:1d
(0)	84:ec:2d:67:f9:c1:7d:79:56:0b:8d:b4:b8:74:30:63
(0)	4c:02:98:d1:6a:0b:76:e9:72:2d:90:78:ac:96:88:a0
(0)	64:04:46:cd:3f:75:64:2a:79:14:a5:88:48:6d:ed:a2
(0)	e5:8b:eb:10:91:9c:05:2a:32:20:d3:d5:a7:d8:16:1d
(0)	4f:c1:91:ed:6d:93:a3:00:8d:b8:26:d0:cc:47:cf:57
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(1)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(1)Valid From	Mar 22 00:00:00 2021 GMT
(1)Valid Till	Mar 21 23:59:59 2036 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(3072 bit)
(1)	RSA Public-Key: (3072 bit)
(1)	Modulus:
(1)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(1)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(1)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(1)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(1)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(1)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(1)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:

(1)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(1)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(1)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(1)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(1)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(1)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(1)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(1)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(1)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(1)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(1)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(1)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(1)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(1)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(1)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(1)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(1)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(1)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(1)	36:d7:77:f5:91:27:08:66:7b:4d
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(1)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	Policy: 2.23.140.1.2.2
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(1)	OCSP - URI:http://ocsp.sectigo.com
(1)Signature	(512 octets)
(1)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(1)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(1)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(1)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(1)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(1)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(1)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(1)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(1)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(1)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(1)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(1)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(1)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(1)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(1)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(1)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(1)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(1)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(1)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88

(1)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(1)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(1)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(1)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(1)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(1)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(1)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(1)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(1)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(1)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(1)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(1)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(1)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(2)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(2)Valid From	Mar 22 00:00:00 2021 GMT
(2)Valid Till	Jan 18 23:59:59 2038 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(2)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(2)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(2)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(2)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(2)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(2)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(2)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(2)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(2)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(2)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(2)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(2)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(2)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(2)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(2)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(2)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(2)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(2)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(2)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(2)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(2)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:

(2)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(2)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(2)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(2)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(2)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(2)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(2)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(2)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(2)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(2)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(2)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(2)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(2)	7c:6d:cf
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(2)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(2)Signature	(512 octets)
(2)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(2)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(2)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(2)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(2)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(2)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(2)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(2)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(2)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(2)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(2)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(2)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(2)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(2)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(2)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(2)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(2)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(2)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(2)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(2)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(2)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(2)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(2)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(2)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(2)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(2)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(2)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc

(2)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(2)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(2)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(2)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(2)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(3)CERTIFICATE 3	
(3)Version	3 (0x2)
(3)Serial Number	01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d
(3)Signature Algorithm	sha384WithRSAEncryption
(3)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)SUBJECT NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)Valid From	Feb 1 00:00:00 2010 GMT
(3)Valid Till	Jan 18 23:59:59 2038 GMT
(3)Public Key Algorithm	rsaEncryption
(3)RSA Public Key	(4096 bit)
(3)	RSA Public-Key: (4096 bit)
(3)	Modulus:
(3)	00:80:12:65:17:36:0e:c3:db:08:b3:d0:ac:57:0d:
(3)	76:ed:cd:27:d3:4c:ad:50:83:61:e2:aa:20:4d:09:
(3)	2d:64:09:dc:ce:89:9f:cc:3d:a9:ec:f6:cf:c1:dc:
(3)	f1:d3:b1:d6:7b:37:28:11:2b:47:da:39:c6:bc:3a:
(3)	19:b4:5f:a6:bd:7d:9d:a3:63:42:b6:76:f2:a9:3b:
(3)	2b:91:f8:e2:6f:d0:ec:16:20:90:09:3e:e2:e8:74:
(3)	c9:18:b4:91:d4:62:64:db:7f:a3:06:f1:88:18:6a:
(3)	90:22:3c:bc:fe:13:f0:87:14:7b:f6:e4:1f:8e:d4:
(3)	e4:51:c6:11:67:46:08:51:cb:86:14:54:3f:bc:33:
(3)	fe:7e:6c:9c:ff:16:9d:18:bd:51:8e:35:a6:a7:66:
(3)	c8:72:67:db:21:66:b1:d4:9b:78:03:c0:50:3a:e8:
(3)	cc:f0:dc:bc:9e:4c:fe:af:05:96:35:1f:57:5a:b7:
(3)	ff:ce:f9:3d:b7:2c:b6:f6:54:dd:c8:e7:12:3a:4d:
(3)	ae:4c:8a:b7:5c:9a:b4:b7:20:3d:ca:7f:22:34:ae:
(3)	7e:3b:68:66:01:44:e7:01:4e:46:53:9b:33:60:f7:
(3)	94:be:53:37:90:73:43:f3:32:c3:53:ef:db:aa:fe:
(3)	74:4e:69:c7:6b:8c:60:93:de:c4:c7:0c:df:e1:32:
(3)	ae:cc:93:3b:51:78:95:67:8b:ee:3d:56:fe:0c:d0:
(3)	69:0f:1b:0f:f3:25:26:6b:33:6d:f7:6e:47:fa:73:
(3)	43:e5:7e:0e:a5:66:b1:29:7c:32:84:63:55:89:c4:
(3)	0d:c1:93:54:30:19:13:ac:d3:7d:37:a7:eb:5d:3a:
(3)	6c:35:5c:db:41:d7:12:da:a9:49:0b:df:d8:80:8a:
(3)	09:93:62:8e:b5:66:cf:25:88:cd:84:b8:b1:3f:a4:
(3)	39:0f:d9:02:9e:eb:12:4c:95:7c:f3:6b:05:a9:5e:
(3)	16:83:cc:b8:67:e2:e8:13:9d:cc:5b:82:d3:4c:b3:
(3)	ed:5b:ff:de:e5:73:ac:23:3b:2d:00:bf:35:55:74:
(3)	09:49:d8:49:58:1a:7f:92:36:e6:51:92:0e:f3:26:
(3)	7d:1c:4d:17:bc:c9:ec:43:26:d0:bf:41:5f:40:a9:

(3)	44:44:f4:99:e7:57:87:9e:50:1f:57:54:a8:3e:fd:
(3)	74:63:2f:b1:50:65:09:e6:58:42:2e:43:1a:4c:b4:
(3)	f0:25:47:59:fa:04:1e:93:d4:26:46:4a:50:81:b2:
(3)	de:be:78:b7:fc:67:15:e1:c9:57:84:1e:0f:63:d6:
(3)	e9:62:ba:d6:5f:55:2e:ea:5c:c6:28:08:04:25:39:
(3)	b8:0e:2b:a9:f2:4c:97:1c:07:3f:0d:52:f5:ed:ef:
(3)	2f:82:0f
(3)	Exponent: 65537 (0x10001)
(3)X509v3 EXTENSIONS	
(3)X509v3 Subject Key Identifier	53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(3)X509v3 Key Usage	critical
(3)	Certificate Sign, CRL Sign
(3)X509v3 Basic Constraints	critical
(3)	CA:TRUE
(3)Signature	(512 octets)
(3)	5c:d4:7c:0d:cf:f7:01:7d:41:99:65:0c:73:c5:52:9f
(3)	cb:f8:cf:99:06:7f:1b:da:43:15:9f:9e:02:55:57:96
(3)	14:f1:52:3c:27:87:94:28:ed:1f:3a:01:37:a2:76:fc
(3)	53:50:c0:84:9b:c6:6b:4e:ba:8c:21:4f:a2:8e:55:62
(3)	91:f3:69:15:d8:bc:88:e3:c4:aa:0b:fd:ef:a8:e9:4b
(3)	55:2a:06:20:6d:55:78:29:19:ee:5f:30:5c:4b:24:11
(3)	55:ff:24:9a:6e:5e:2a:2b:ee:0b:4d:9f:7f:f7:01:38
(3)	94:14:95:43:07:09:fb:60:a9:ee:1c:ab:12:8c:a0:9a
(3)	5e:a7:98:6a:59:6d:8b:3f:08:fb:c8:d1:45:af:18:15
(3)	64:90:12:0f:73:28:2e:c5:e2:24:4e:fc:58:ec:f0:f4
(3)	45:fe:22:b3:eb:2f:8e:d2:d9:45:61:05:c1:97:6f:a8
(3)	76:72:8f:8b:8c:36:af:bf:0d:05:ce:71:8d:e6:a6:6f
(3)	1f:6c:a6:71:62:c5:d8:d0:83:72:0c:f1:67:11:89:0c
(3)	9c:13:4c:72:34:df:bc:d5:71:df:aa:71:dd:e1:b9:6c
(3)	8c:3c:12:5d:65:da:bd:57:12:b6:43:6b:ff:e5:de:4d
(3)	66:11:51:cf:99:ae:ec:17:b6:e8:71:91:8c:de:49:fe
(3)	dd:35:71:a2:15:27:94:1c:cf:61:e3:26:bb:6f:a3:67
(3)	25:21:5d:e6:dd:1d:0b:2e:68:1b:3b:82:af:ec:83:67
(3)	85:d4:98:51:74:b1:b9:99:80:89:ff:7f:78:19:5c:79
(3)	4a:60:2e:92:40:ae:4c:37:2a:2c:c9:c7:62:c8:0e:5d
(3)	f7:36:5b:ca:e0:25:25:01:b4:dd:1a:07:9c:77:00:3f
(3)	d0:dc:d5:ec:3d:d4:fa:bb:3f:cc:85:d6:6f:7f:a9:2d
(3)	df:b9:02:f7:f5:97:9a:b5:35:da:c3:67:b0:87:4a:a9
(3)	28:9e:23:8e:ff:5c:27:6b:e1:b0:4f:f3:07:ee:00:2e
(3)	d4:59:87:cb:52:41:95:ea:f4:47:d7:ee:64:41:55:7c
(3)	8d:59:02:95:dd:62:9d:c2:b9:ee:5a:28:74:84:a5:9b
(3)	b7:90:c7:0c:07:df:f5:89:36:74:32:d6:28:c1:b0:b0
(3)	0b:e0:9c:4c:c3:1c:d6:fc:e3:69:b5:47:46:81:2f:a2
(3)	82:ab:d3:63:44:70:c4:8d:ff:2d:33:ba:ad:8f:7b:b5
(3)	70:88:ae:3e:19:cf:40:28:d8:fc:c8:90:bb:5d:99:22
(3)	f5:52:e6:58:c5:1f:88:31:43:ee:88:1d:d7:c6:8e:3c
(3)	43:6a:1d:a7:18:de:7d:3d:16:f1:62:f9:ca:90:a8:fd
(4)CERTIFICATE 4	
(4)Version	3 (0x2)
(4)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(4)Signature Algorithm	sha384WithRSAEncryption
(4)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City

organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(4)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(4)Valid From	Mar 22 00:00:00 2021 GMT
(4)Valid Till	Jan 18 23:59:59 2038 GMT
(4)Public Key Algorithm	rsaEncryption
(4)RSA Public Key	(4096 bit)
(4)	RSA Public-Key: (4096 bit)
(4)	Modulus:
(4)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(4)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(4)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(4)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(4)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(4)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(4)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(4)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(4)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(4)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(4)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(4)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(4)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(4)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(4)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(4)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(4)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(4)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(4)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(4)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(4)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(4)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(4)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(4)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(4)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(4)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(4)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(4)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(4)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(4)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(4)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(4)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(4)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(4)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(4)	7c:6d:cf
(4)	Exponent: 65537 (0x10001)
(4)X509v3 EXTENSIONS	
(4)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(4)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(4)X509v3 Key Usage	critical
(4)	Digital Signature, Certificate Sign, CRL Sign
(4)X509v3 Basic Constraints	critical
(4)	CA:TRUE

(4)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(4)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(4)X509v3 CRL Distribution Points	
(4)	Full Name:
(4)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(4)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(4)Signature	(512 octets)
(4)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(4)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(4)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(4)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(4)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(4)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(4)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(4)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(4)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(4)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(4)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(4)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(4)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(4)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(4)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(4)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(4)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(4)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(4)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(4)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(4)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(4)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(4)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(4)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(4)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(4)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(4)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(4)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(4)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(4)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(4)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(4)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(5)CERTIFICATE 5	
(5)Version	3 (0x2)
(5)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(5)Signature Algorithm	sha384WithRSAEncryption
(5)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(5)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(5)Valid From	Mar 22 00:00:00 2021 GMT
(5)Valid Till	Mar 21 23:59:59 2036 GMT
(5)Public Key Algorithm	rsaEncryption
(5)RSA Public Key	(3072 bit)

(5)	RSA Public-Key: (3072 bit)
(5)	Modulus:
(5)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(5)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(5)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(5)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(5)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(5)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(5)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(5)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(5)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(5)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(5)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(5)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(5)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(5)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(5)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(5)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(5)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(5)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(5)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(5)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(5)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(5)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(5)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(5)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(5)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(5)	36:d7:77:f5:91:27:08:66:7b:4d
(5)	Exponent: 65537 (0x10001)
(5)	X509v3 EXTENSIONS
(5)	X509v3 Authority Key Identifier keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(5)	X509v3 Subject Key Identifier E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(5)	X509v3 Key Usage critical
(5)	Digital Signature, Certificate Sign, CRL Sign
(5)	X509v3 Basic Constraints critical
(5)	CA:TRUE, pathlen:0
(5)	X509v3 Extended Key Usage TLS Web Server Authentication, TLS Web Client Authentication
(5)	X509v3 Certificate Policies Policy: X509v3 Any Policy
(5)	Policy: 2.23.140.1.2.2
(5)	X509v3 CRL Distribution Points
(5)	Full Name:
(5)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(5)	Authority Information Access CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(5)	OCSP - URI:http://ocsp.sectigo.com
(5)	Signature (512 octets)
(5)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(5)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(5)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(5)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(5)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(5)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(5)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(5)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(5)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(5)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87

(5)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(5)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(5)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(5)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(5)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(5)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(5)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(5)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(5)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(5)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(5)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(5)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(5)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(5)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(5)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(5)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(5)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(5)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(5)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(5)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(5)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(5)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c

1 Web Server Supports HTTP Request Pipelining

port 8090/tcp over SSL

QID: 86565
 Category: Web server
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 02/22/2005
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:8090

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:8090

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:39:59 GMT
Content-Type: text/html
Content-Length: 6718
Last-Modified: Mon, 13 Apr 2026 16:24:55 GMT
Connection: keep-alive
ETag: "69dd18d7-1a3e"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

```
<!DOCTYPE html>  
<html lang="es">
```

```
<head>  
  <meta charset="UTF-8">  
  <title>Chat Eureka</title>  
  <link href="https://fonts.googleapis.com/css2?family=Nunito+Sans:wght@400;600;700;800&display=swap" rel="stylesheet">  
  <link rel="stylesheet" href="style.css">  
</head>
```

```
<body>
```

```
<!-- Overlay de T_C3_A9rminos y Condiciones (sin cambios) -->  
<div id="terms_overlay" class="terms-overlay" role="dialog" aria-modal="true" aria-labelledby="terms_title">  
  <div class="terms-card">  
    <h2 id="terms_title">T_C3_A9rminos y Condiciones</h2>  
    <div class="terms-content" id="terms_content">  
      <pre>  
        T_C3_A9rminos y Condiciones de Uso y Aviso de Privacidad del Chatbot Eureka 2.0 ANLA  
        Bienvenido al chatbot informativo de Eureka 2.0 ANLA
```

Antes de utilizar este servicio, es fundamental que lea, comprenda y acepte los siguientes t_C3_A9rminos y condiciones que regulan su uso. El acceso y utilizaci_C3_B3n de este chatbot implica la aceptaci_C3_B3n expresa de las cl_C3_A1usulas que se detallan a continuaci_C3_B3n.

1. Naturaleza y Alcance del Servicio

Car_C3_A1cter meramente informativo: Las respuestas que ofrece este chatbot tienen un prop_C3_B3sito exclusivamente orientativo. Se sustentan en documentaci_C3_B3n p_C3_BAblica y oficial disponible, pero no deben considerarse completas ni definitivas.

Uso de inteligencia artificial: Este chatbot funciona mediante modelos de inteligencia artificial que procesan la informaci_C3_B3n suministrada por el usuario. Por ello, las respuestas pueden contener imprecisiones o interpretaciones aproximadas y deben ser verificadas antes de adoptar decisiones.

No constituye asesor_C3_ADa legal ni t_C3_A9cnica: La informaci_C3_B3n aqu_C3_AD proporcionada no reemplaza el an_C3_A1lisis, la interpretaci_C3_B3n ni la asesor_C3_ADa de profesionales cualificados. En ning_C3_BAn caso podr_C3_A1 entenderse como una opini_C3_B3n vinculante de la ANLA. Para consultas con validez jur_C3_ADdica o t_C3_A9cnica, se recomienda acudir a un experto y/o a los canales oficiales de la Entidad.

Herramienta complementaria: Este chatbot es un canal de apoyo informativo y no sustituye los mecanismos formales de atenci_C3_B3n al ciudadano. No tiene capacidad para tramitar solicitudes, responder PQRSD (Peticiones, Quejas, Reclamos, Sugerencias y Denuncias) ni gestionar radicaciones. Para estos fines deber_C3_A1 acudir exclusivamente a los canales oficiales de la ANLA.

2. Limitaciones del Contenido

El sistema est_C3_A1 programado para no procesar ni responder a consultas relacionadas con:

Informaci_C3_B3n sobre expedientes, licencias, permisos o tr_C3_A1mites espec_C3_ADficos en curso.

Datos personales o sensibles del usuario o de terceros.

Programaci_C3_B3n o detalles log_C3_ADsticos de audiencias p_C3_BAblicas, reuniones o eventos.

Opiniones, valoraciones subjetivas o juicios de valor.

3. Validaci_C3_B3n y Seguridad de la Informaci_C3_B3n

Contraste con fuentes oficiales: Por motivos de seguridad y confiabilidad, se recomienda verificar toda la informaci_C3_B3n proporcionada en este chatbot directamente en la plataforma oficial Eureka 2.0 u otros canales oficiales de la ANLA.

Limitaciones propias de la IA: Debido al estado actual de la tecnolog_C3_ADa, el chatbot puede, en casos aislados, generar errores u ofrecer informaci_C3_B3n imprecisa (_E2_80_9Calucinaciones_E2_80_9D). Por esta raz_C3_B3n, se insiste en la necesidad de validar siempre los datos en las fuentes oficiales.

4. Pol_C3_ADtica de Privacidad y Mejora Continua

La interacci_C3_B3n con el chatbot podr_C3_A1 ser utilizada con fines de an_C3_A1lisis estad_C3_ADstico y mejora del servicio.

Esta informaci_C3_B3n se recopil_C3_A1 de manera an_C3_B3nima, sin almacenar datos personales identificables (como nombres, n_C3_BAmoros de identificaci_C3_B3n o correos electr_C3_B3nicos).

La retroalimentaci_C3_B3n de los usuarios es esencial para optimizar la calidad de la herramienta, siempre dentro de par_C3_A1metros de seguridad y confidencialidad.

5. Exclusi_C3_B3n de Responsabilidad

La ANLA no asume responsabilidad alguna por:

Las decisiones adoptadas por los usuarios con base en la informaci_C3_B3n suministrada por el chatbot.

Cualquier error, inconsistencia o falta de actualizaci_C3_B3n de la informaci_C3_B3n generada por el sistema.

El uso indebido del chatbot o la interpretaci_C3_B3n err_C3_B3nea de las respuestas.

6. Aceptaci_C3_B3n de los T_C3_A9rminos

El inicio de la conversaci_C3_B3n con el chatbot constituye prueba de que el usuario ha le_C3_ADdo, comprendido y aceptado estos T_C3_A9rminos y Condiciones. Si no est_C3_A1 de acuerdo con ellos, le solicitamos abstenerse de utilizar este servicio.

```
</pre>
```

```
</div>
```

```
<div class="terms-actions">
```

```
<button id="accept_btn" class="btn primary">Acepto</button>
```

```
<button id="decline_btn" class="btn danger">No acepto</button>
```

```
</div>
```

```
</div>
```

```
</div>
```

```
<div id="chat_app">
```

```
<main>
```

```
<header class="anla-header">
```

```

```

```
<a href="https://www.anla.gov.co/07rediseureka2024" target="_blank">
```

```

```

```
</a>
```

```
</header>
```

```
<h1>Chat Eureka</h1>
```

```
<div class="chat-container">
```

```
<div id="chat_response">
```

```
<div class="welcome-message">_C2_A1Hola! Soy Eureka, tu asistente virtual. _C2_BFEn qu_C3_A9 puedo ayudarte hoy?</div>
```

```
</div>
```

```
</div>
```

```
</main>
```

```
<form onsubmit="sendMessage(event)">
```

```
<input type="text" id="messageText" placeholder="Escribe tu pregunta_E2_80_A6" aria-label="Tu pregunta para Eureka" />
```

```
<button type="submit">Enviar</button>
```

```
<!-- _F0_9F_94_8A Bot_C3_B3n TTS -->
```

```
<button type="button" id="speak_btn" class="speak-btn" aria-label="Escuchar respuesta" title="Escuchar respuesta">
```

```
_F0_9F_94_8A Escuchar
```

```
</button>
```

```
</form>
```

```
<footer class="site-footer" aria-hidden="true">
```

```
_C2_A9 Copyright 2020 Herramienta de consulta EUREKA!!
```

```
Todos los derechos reservados Gobierno de Colombia - ANLA
```

```
</footer>
```

```
</div> <!-- /#chat_app -->
```

```
<!-- _E2_9A_A0_EF_B8_8F NUEVO: mensaje cuando el usuario NO acepta -->
```

```
<div id="blocked" class="blocked" hidden aria-live="polite">
```

```
<div class="blocked-card">
```

```
<h2>Acceso no permitido</h2>
```

```
<p>No se puede acceder al chatbot si no se aceptan los T_C3_A9rminos y Condiciones.</p>
```

```
</div>
```

```
</div>
```

```
<script src="script.js"></script>
```

```
</body>
```

```
</html>
```

HTTP/1.1 404 Not Found
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:39:59 GMT
Content-Type: text/html
Content-Length: 153
Connection: keep-alive

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.29.8</center>
</body>
</html>
```



1 Default Web Page

port 8443/tcp over SSL

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.25.4
Date: Sat, 25 Apr 2026 00:27:59 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT
Connection: keep-alive
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *

Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Accept, Authorization, Cache-Control, Content-Type, DNT, If-Modified-Since, Keep-Alive, Origin, User-Agent, X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>

<body>

  <script type="module">
    import Chatbot from "https://cdn.jsdelivr.net/npm/flowise-embed/dist/web.js"
    Chatbot.init({
      chatflowid: "5e1b245a-0c47-45fc-a1c5-d2f10d475478",
      apiHost: "https://172.40.123.5:8000",
    })
  </script>

</body>

</html>
```



1 Default Web Page (Follow HTTP Redirection)

port 8443/tcp over SSL

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8443
Connection: Keep-Alive

```
HTTP/1.1 200 OK
Server: nginx/1.25.4
Date: Sat, 25 Apr 2026 00:31:05 GMT
Content-Type: text/html
Content-Length: 479
Last-Modified: Wed, 10 Sep 2025 03:27:34 GMT
Connection: keep-alive
ETag: "68c0f026-1df"
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-Alive,Origin,User-Agent,X-Requested-With
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Accept-Ranges: bytes

<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>

<body>

  <script type="module">
    import Chatbot from "https://cdn.jsdelivr.net/npm/flowise-embed/dist/web.js"
    Chatbot.init({
      chatflowid: "5e1b245a-0c47-45fc-a1c5-d2f10d475478",
      apiHost: "https://172.40.123.5:8000",
    })
  </script>

</body>

</html>
```



1 SSL Server Information Retrieval

port 8443/tcp over SSL

QID:	38116
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
CAMELLIA128-SHA256	RSA	RSA	SHA256	Camellia(128)	MEDIUM
CAMELLIA256-SHA256	RSA	RSA	SHA256	Camellia(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ARIA128-GCM-SHA256	RSA	RSA	AEAD	ARIAGCM(128)	MEDIUM
ARIA256-GCM-SHA384	RSA	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-ARIA128-GCM-SHA256	ECDH	RSA	AEAD	ARIAGCM(128)	MEDIUM
ECDHE-RSA-ARIA256-GCM-SHA384	ECDH	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-CAMELLIA128-SHA256	ECDH	RSA	SHA256	Camellia(128)	MEDIUM
ECDHE-RSA-CAMELLIA256-SHA384	ECDH	RSA	SHA384	Camellia(256)	HIGH
AES128-CCM	RSA	RSA	AEAD	AESCCM(128)	MEDIUM
AES256-CCM	RSA	RSA	AEAD	AESCCM(256)	HIGH
AES128-CCM-8	RSA	RSA	AEAD	AESCCM8(128)	MEDIUM
AES256-CCM-8	RSA	RSA	AEAD	AESCCM8(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH



QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 8443/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303



1 SSL Certificate will expire within next six months

port 8443/tcp over SSL

QID: 38600
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/14/2024
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=172.40.123.5,O=LocalDev,L=Bogota,ST=Cundinamarca,C=CO The certificate will expire within six months: Sep 9 15:43:58 2026 GMT



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 8443/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
AES256-SHA256	RSA		2048	no	110	low
AES128-SHA256	RSA		2048	no	110	low
AES256-CCM-8	RSA		2048	no	110	low
AES128-CCM-8	RSA		2048	no	110	low
AES256-CCM	RSA		2048	no	110	low
AES128-CCM	RSA		2048	no	110	low
ARIA256-GCM-SHA384	RSA		2048	no	110	low
ARIA128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA256	RSA		2048	no	110	low
AES256-GCM-SHA384	RSA		2048	no	110	low
AES128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA	RSA		2048	no	110	low
CAMELLIA128-SHA	RSA		2048	no	110	low
AES256-SHA	RSA		2048	no	110	low
AES128-SHA	RSA		2048	no	110	low
CAMELLIA128-SHA256	RSA		2048	no	110	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low

ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low

TLSv1.3

TLS13-AES-128-GCM-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe8192	8192	yes	202	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe2048	2048	yes	110	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe3072	3072	yes	132	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe4096	4096	yes	150	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe6144	6144	yes	178	low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe8192	8192	yes	202	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe2048	2048	yes	110	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe3072	3072	yes	132	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe4096	4096	yes	150	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe6144	6144	yes	178	low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe8192	8192	yes	202	low
TLS13-AES-128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-128-GCM-SHA256	ECDHE	x448	448	yes	224	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
TLS13-AES-256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
TLS13-AES-256-GCM-SHA384	ECDHE	x448	448	yes	224	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
TLS13-AES-256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x25519	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp256r1	256	yes	128	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	x448	448	yes	224	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp521r1	521	yes	260	low
TLS13-CHACHA20-POLY1305-SHA256	ECDHE	secp384r1	384	yes	192	low



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 8443/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

1 TLS Secure Renegotiation Extension Support Information

port 8443/tcp over SSL

QID: 42350
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the

client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierrenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 8443/tcp over SSL

QID:	48340
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	SSL/TLS Server supports TLSv1.2
Bugtraq ID:	-
Service Modified:	04/13/2026
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 8443/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	33:50:9c:f8:c0:cb:4b:4b:eb:10:7a:d8:a8:4f:46:35:5b:e6:18:89
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	CO
stateOrProvinceName	Cundinamarca
localityName	Bogota
organizationName	LocalDev
commonName	172.40.123.5
(0)SUBJECT NAME	
countryName	CO
stateOrProvinceName	Cundinamarca
localityName	Bogota
organizationName	LocalDev
commonName	172.40.123.5
(0)Valid From	Sep 9 15:43:58 2025 GMT
(0)Valid Till	Sep 9 15:43:58 2026 GMT

(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:ae:3a:aa:6f:80:bc:8a:fc:03:f8:07:f5:6d:f2:
(0)	e0:3c:4e:94:6d:a3:c6:5e:d0:17:26:05:b0:89:dd:
(0)	56:2d:be:07:fd:27:2d:da:ad:b8:49:9e:20:fc:95:
(0)	73:4d:d4:29:16:13:1d:d6:d4:32:e5:1d:b7:75:6f:
(0)	99:10:c5:a3:d6:8d:c6:7b:5f:26:36:cc:30:4f:92:
(0)	df:2f:61:10:59:63:02:f0:f6:8f:00:e1:c6:49:d4:
(0)	c1:8e:67:60:8d:f4:bc:c3:29:b9:90:fe:46:0b:ef:
(0)	ae:45:da:18:77:a6:d8:a3:35:ad:51:8e:4e:92:bb:
(0)	b5:e9:c6:85:4a:73:1a:6b:20:9b:9d:2d:d8:f4:10:
(0)	3f:ea:c5:ba:93:92:5c:1d:28:ec:ac:4e:2e:cb:b0:
(0)	25:ea:50:dc:3a:c4:75:b8:e2:ed:22:62:a0:97:41:
(0)	b3:7a:65:20:5a:05:af:0d:d6:5c:28:48:9e:e5:33:
(0)	79:2c:25:27:d2:03:cd:03:6f:58:1d:63:5c:9e:c6:
(0)	7d:00:8c:0b:1d:4b:5f:43:83:3b:74:8b:00:e8:ac:
(0)	ff:50:b6:f0:15:da:21:8a:13:d6:5a:0f:92:0a:8d:
(0)	b9:7e:c1:2d:95:01:2f:fb:3b:cd:47:2f:d4:93:22:
(0)	e7:79:0a:cb:1e:b7:35:19:00:ce:50:24:74:30:14:
(0)	92:1d
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Subject Key Identifier	23:FB:64:35:56:78:5F:F8:7D:96:DA:92:D3:F3:30:CC:A8:6D:F3:99
(0)X509v3 Authority Key Identifier	keyid:23:FB:64:35:56:78:5F:F8:7D:96:DA:92:D3:F3:30:CC:A8:6D:F3:99
(0)X509v3 Basic Constraints	critical
(0)	CA:TRUE
(0)Signature	(256 octets)
(0)	09:c2:a9:1c:f1:49:17:07:a3:1c:f6:0c:b1:4f:e6:eb
(0)	9c:3c:e0:cd:cb:17:c7:05:28:52:49:d9:64:d9:9b:6b
(0)	90:c4:74:5c:f5:07:08:c8:a8:8a:a2:06:19:a9:91:6e
(0)	a1:9a:9f:ed:f3:2d:eb:32:6c:9f:bc:f5:ad:90:ad:8f
(0)	f3:45:eb:68:5d:0b:7d:25:dd:9a:e0:67:a2:f1:a4:7d
(0)	c4:75:96:71:27:8d:c9:b5:2a:ba:d4:8e:d6:6e:84:8e
(0)	b3:52:86:73:4f:ad:6b:05:83:99:d3:b7:b5:9a:e4:c2
(0)	0e:7d:a2:d9:45:cf:0d:dc:93:3c:b4:2e:0f:a6:bf:ba
(0)	ae:87:b1:d8:f6:4d:59:6d:09:51:e2:68:12:c0:72:17
(0)	2e:6d:eb:9c:c6:c8:39:7b:15:81:32:e5:f0:01:b9:c9
(0)	cb:55:2f:ab:79:41:bb:b3:93:0b:f2:e2:78:58:c9:08
(0)	51:b4:cc:8f:fb:01:c2:de:62:ae:56:6d:99:7c:f7:a9
(0)	b6:b0:aa:a3:81:4b:e2:bc:4f:8d:dc:61:c7:1f:02:f0
(0)	d4:5f:34:e8:be:52:c0:9f:3c:ce:a5:73:1e:f7:36:09
(0)	87:cf:29:8e:cd:36:87:43:6c:cc:d5:20:0a:c7:ea:83
(0)	af:51:34:80:89:f8:eb:f7:c8:69:d6:f7:8b:00:ec:1f

 1 Default Web Page

port 3000/tcp

QID: 12230
 Category: CGI
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/15/2019
 User Modified: -

Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:3000
Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Flowise - Build AI Agents, Visually</title>
    <link rel="icon" href="favicon.ico" />
    <!-- Meta Tags-->
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="theme-color" content="#2296f3" />
    <meta name="title" content="Flowise - Build AI Agents, Visually" />
    <meta
      name="description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <link rel="manifest" href="manifest.json" />
    <link rel="apple-touch-icon" href="logo192.png" />
    <meta name="keywords" content="react, material-ui, workflow automation, llm, artificial-intelligence" />
    <meta name="author" content="FlowiseAI" />
    <!-- Open Graph / Facebook -->
    <meta property="og:locale" content="en_US" />
    <meta property="og:type" content="website" />
    <meta property="og:url" content="https://flowiseai.com/" />
    <meta property="og:site_name" content="flowiseai.com" />
    <meta property="og:title" content="Flowise - Build AI Agents, Visually" />
    <meta
      property="og:description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <!-- Twitter -->
    <meta property="twitter:card" content="summary_large_image" />
    <meta property="twitter:url" content="https://twitter.com/FlowiseAI" />
    <meta property="twitter:title" content="Flowise - Build AI Agents, Visually" />
    <meta
      property="twitter:description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <meta name="twitter:creator" content="@FlowiseAI" />
```

```

<link rel="preconnect" href="https://fonts.gstatic.com" />
<link
href="https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap"
rel="stylesheet"
/>
<script>
;(function (w, r) {
  w._rwq = r
  w[r] =
    w[r] ||
    function () {
      ;(w[r].q = w[r].q || []).push(arguments)
    }
})(window, 'rewardful')
</script>
<script async src="https://r.wdfl.co/rw.js" data-rewardful="9a3a26"></script>
<script type="module" crossorigin src="/assets/index-C6GKaUTA.js"></script>
<link rel="stylesheet" crossorigin href="/assets/index-9xw-RjBM.css">
</head>

<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root"></div>
<div id="portal"></div>
<script>
  if (global === undefined) {
    var global = window
  }
</script>
</body>
</html>

```

1 Default Web Page (Follow HTTP Redirection)

port 3000/tcp

QID: 13910
 Category: CGI
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 11/05/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:3000
Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Flowise - Build AI Agents, Visually</title>
    <link rel="icon" href="favicon.ico" />
    <!-- Meta Tags-->
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="theme-color" content="#2296f3" />
    <meta name="title" content="Flowise - Build AI Agents, Visually" />
    <meta
      name="description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <link rel="manifest" href="manifest.json" />
    <link rel="apple-touch-icon" href="logo192.png" />
    <meta name="keywords" content="react, material-ui, workflow automation, llm, artificial-intelligence" />
    <meta name="author" content="FlowiseAI" />
    <!-- Open Graph / Facebook -->
    <meta property="og:locale" content="en_US" />
    <meta property="og:type" content="website" />
    <meta property="og:url" content="https://flowiseai.com/" />
    <meta property="og:site_name" content="flowiseai.com" />
    <meta property="og:title" content="Flowise - Build AI Agents, Visually" />
    <meta
      property="og:description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <!-- Twitter -->
    <meta property="twitter:card" content="summary_large_image" />
    <meta property="twitter:url" content="https://twitter.com/FlowiseAI" />
    <meta property="twitter:title" content="Flowise - Build AI Agents, Visually" />
    <meta
      property="twitter:description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <meta name="twitter:creator" content="@FlowiseAI" />

    <link rel="preconnect" href="https://fonts.gstatic.com" />
    <link
      href="https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap"
      rel="stylesheet"
    />
    <script>
      ;(function (w, r) {
        w._rwq = r
        w[r] =
          w[r] ||
          function () {
            ;(w[r].q = w[r].q || []).push(arguments)
          }
      })(window, 'rewardful')
    </script>
    <script async src="https://r.wdf.l.co/rw.js" data-rewardful="9a3a26"></script>
    <script type="module" crossorigin src="/assets/index-C6GKaUTA.js"></script>
    <link rel="stylesheet" crossorigin href="/assets/index-9xw-RjBM.css">
  </head>

  <body>
    <noscript>You need to enable JavaScript to run this app.</noscript>
    <div id="root"></div>
    <div id="portal"></div>
    <script>
      if (global === undefined) {
        var global = window
      }
    </script>
  </body>
</html>
```



1 HTTP Response Method and Header Information Collected

port 3000/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 3000.

GET / HTTP/1.1
Host: 172.40.123.5:3000
Connection: Keep-Alive

HTTP/1.1 200 OK
Vary: Origin
Content-Security-Policy: frame-ancestors
Access-Control-Allow-Credentials: true
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 11 Aug 2025 12:14:01 GMT
ETag: W/"c46-198990d4728"
Content-Type: text/html; charset=UTF-8
Content-Length: 3142
Date: Sat, 25 Apr 2026 01:08:27 GMT
Connection: keep-alive
Keep-Alive: timeout=5



1 Referrer-Policy HTTP Security Header Not Detected

port 3000/tcp

QID: 48131
Category: Information gathering

Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 3000 port.
GET / HTTP/1.1
Host: 172.40.123.5:3000
Connection: Keep-Alive

1 Web Server Supports HTTP Request Pipelining

port 3000/tcp

QID: 86565
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/22/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:3000

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:3000

HTTP/1.1 200 OK
Vary: Origin
Content-Security-Policy: frame-ancestors
Access-Control-Allow-Credentials: true
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 11 Aug 2025 12:14:01 GMT
ETag: W/"c46-198990d4728"
Content-Type: text/html; charset=UTF-8
Content-Length: 3142
Date: Sat, 25 Apr 2026 02:41:10 GMT
Connection: keep-alive
Keep-Alive: timeout=5

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Flowise - Build AI Agents, Visually</title>
    <link rel="icon" href="favicon.ico" />
    <!-- Meta Tags-->
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="theme-color" content="#2296f3" />
    <meta name="title" content="Flowise - Build AI Agents, Visually" />
    <meta
      name="description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <link rel="manifest" href="manifest.json" />
    <link rel="apple-touch-icon" href="logo192.png" />
    <meta name="keywords" content="react, material-ui, workflow automation, llm, artificial-intelligence" />
    <meta name="author" content="FlowiseAI" />
    <!-- Open Graph / Facebook -->
    <meta property="og:locale" content="en_US" />
    <meta property="og:type" content="website" />
    <meta property="og:url" content="https://flowiseai.com/" />
    <meta property="og:site_name" content="flowiseai.com" />
```

```

<meta property="og:title" content="Flowise - Build AI Agents, Visually" />
<meta
  property="og:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<!-- Twitter -->
<meta property="twitter:card" content="summary_large_image" />
<meta property="twitter:url" content="https://twitter.com/FlowiseAI" />
<meta property="twitter:title" content="Flowise - Build AI Agents, Visually" />
<meta
  property="twitter:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<meta name="twitter:creator" content="@FlowiseAI" />

<link rel="preconnect" href="https://fonts.gstatic.com" />
<link
  href="https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap"
  rel="stylesheet"
/>
<script>
;(function (w, r) {
  w._rwq = r
  w[r] =
    w[r] ||
    function () {
      ;(w[r].q = w[r].q || []).push(arguments)
    }
})(window, 'rewardful')
</script>
<script async src="https://r.wdfl.co/rw.js" data-rewardful="9a3a26"></script>
<script type="module" crossorigin src="/assets/index-C6GKaUTA.js"></script>
<link rel="stylesheet" crossorigin href="/assets/index-9xw-RjBM.css">
</head>

<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root"></div>
<div id="portal"></div>
<script>
  if (global === undefined) {
    var global = window
  }
</script>
</body>
</html>
HTTP/1.1 200 OK
Vary: Origin
Content-Security-Policy: frame-ancestors
Access-Control-Allow-Credentials: true
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 11 Aug 2025 12:14:01 GMT
ETag: W/"c46-198990d4728"
Content-Type: text/html; charset=UTF-8
Content-Length: 3142
Date: Sat, 25 Apr 2026 02:41:10 GMT
Connection: keep-alive
Keep-Alive: timeout=5

<!DOCTYPE html>
<html lang="en">
<head>
<title>Flowise - Build AI Agents, Visually</title>
<link rel="icon" href="favicon.ico" />
<!-- Meta Tags-->
<meta charset="utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<meta name="theme-color" content="#2296f3" />
<meta name="title" content="Flowise - Build AI Agents, Visually" />
<meta
  name="description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<link rel="manifest" href="manifest.json" />
<link rel="apple-touch-icon" href="logo192.png" />
<meta name="keywords" content="react, material-ui, workflow automation, llm, artificial-intelligence" />

```

```

<meta name="author" content="FlowiseAI" />
<!-- Open Graph / Facebook -->
<meta property="og:locale" content="en_US" />
<meta property="og:type" content="website" />
<meta property="og:url" content="https://flowiseai.com/" />
<meta property="og:site_name" content="flowiseai.com" />
<meta property="og:title" content="Flowise - Build AI Agents, Visually" />
<meta
  property="og:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<!-- Twitter -->
<meta property="twitter:card" content="summary_large_image" />
<meta property="twitter:url" content="https://twitter.com/FlowiseAI" />
<meta property="twitter:title" content="Flowise - Build AI Agents, Visually" />
<meta
  property="twitter:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<meta name="twitter:creator" content="@FlowiseAI" />

<link rel="preconnect" href="https://fonts.gstatic.com" />
<link
href="https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap"
rel="stylesheet"
/>
<script>
;(function (w, r) {
  w._rwq = r
  w[r] =
    w[r] ||
    function () {
      ;(w[r].q = w[r].q || []).push(arguments)
    }
})(window, 'rewardful')
</script>
<script async src="https://r.wdfl.co/rw.js" data-rewardful="9a3a26"></script>
<script type="module" crossorigin src="/assets/index-C6GKaUTA.js"></script>
<link rel="stylesheet" crossorigin href="/assets/index-9xw-RjBM.css">
</head>

<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root"></div>
<div id="portal"></div>
<script>
  if (global === undefined) {
    var global = window
  }
</script>
</body>
</html>

```

1 List of Web Directories

port 3000/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/assets/	web page



1 Apache Default Foreign Language File Still on Server

port 3000/tcp

QID: 86743
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/11/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Apache installs foreign language files along with index.html. The files are as follows:

index.html.ca
index.html.de
index.html.dk
index.html.ee

An attacker can get additional information about the Web server from these files.

IMPACT:

Sensitive system information may be disclosed, which can be utilized by an attacker to aid further attacks.

SOLUTION:

Apache recommends to remove these files from the Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /index.html.ru.iso-ru HTTP/1.1
Host: 172.40.123.5:3000
Connection: Keep-Alive



1 Default Web Page

port 9443/tcp over SSL

QID: 12230
Category: CGI

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:9443
Connection: Keep-Alive

```
<!doctype html><html lang="en" ng-app="portainer" ng-strict-di data-edition="CE"><head><meta
charset="utf-8"/><title>Portainer</title><meta name="description" content=""/><meta name="author"
content="Portainer.io"/><meta http-equiv="cache-control" content="no-cache"/><meta http-equiv="expires"
content="0"/><meta http-equiv="pragma" content="no-cache"/><meta name="robots" content="noindex"/><base
id="base"/><script>if (window.origin == 'file://') {
  // we are loading the app from a local file as in docker extension
  document.getElementById('base').href = 'http://localhost:49000/';

  window.ddExtension = true;
} else {
  var path = window.location.pathname.replace(/^V+|V+$/g, '');
  var basePath = path ? '/' + path + '/' : '/';
  document.getElementById('base').href = basePath;
}</script><!--[if lt IE 9]>
<script src="//html5shim.googlecode.com/svn/trunk/html5.js"></script>
<![endif]><link rel="apple-touch-icon" sizes="180x180" href="63a301f0574f1a696ce6.png"/><link rel="icon"
type="image/png" sizes="32x32" href="2dcfc527d067d4ae3424.png"/><link rel="icon" type="image/png" sizes="16x16"
href="112a479c093f4729251d.png"/><link rel="mask-icon"
href="data:image/svg+xml;base64,PHN2ZyB2ZXJzaW9uPSIxliB4bWxuc20iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmcilHdpZHRoPSI0MjAilGh
laWdodD0iNDIwliB2aWV3Qm94PSIwIDAgMzE1LjAwMDAwMCAzMtUuMDAwMDAwlj48cGF0aCBkPSJNMtYzIIEzLjN2Ni40bC0zOC4zIDlyLjEtMzguMiAyMi
4xaC0zNGMtMi44LjEtMyAuMy0zLjIlgNC41LS4yIDMuNC4xIDQuNSAxLjUgNC40LjkuMiAxNiAuMyAzMy41LjIlgMTcuNCAwIDMxLjcuMiAzMS44LjUuMS4zL
jIlgMTAuMy40IDlyLjEuMSAxMS44LjMgMjEuOC40IDlyLjIlgMCAuNSA1LjUuOCAXMiAuOGxMS45bC0uMS0yMi44LS4xLTlyLjcgMTEuMi0uMUgXNjNWwMjA0
bDMuNS4xYzEuOS4xIDQuMS4yIDQuNy4zIDIEgljEgMS4zLTEzLjcgMS4zLTY1LjNWwNzMuN2wzLjMtLjMgMy4yLS4yLjEgNjYuNnY2Ni43bDQuOCAXLjEgNC4
3IDMuMnYtNjIjLS4xLTM4IC4xLTY5LjMuNC02OS43LjMtLjQgMTcuMi0uNy4zLjEgMS43aDM3bC4zLTQuNi4zLTQuNi04LjMtLjMtOC4zLS40LTM3LTlxLj
RjLTIwLjMtMTEuOC0zNy4yLTlxLjYtMzcuNS0yMS44LS4zLS4zLS41LTluOC0uNi01LjYtLjEtMi45LS4yLTUuOC0uMy02LjUtLjEtLjctMS43LTEuMi00L
jYtMS4ySDE2M3Y2LjN6bTAgMzQuMXyXNi41aC0yOC4yYy0yOCAXLTi4LjMgMC0yNS44LTEuOSAXLjQtMSA0LjMtMi44IDYUNs00IDluMi0xLjEgMTMuNS03
LjYgMjUuMTQuNCAxMS42LTYuOSAYMS4zLTEyLjUgMjEuOC0xMi41LjQtLjEuNyA3LjMuNyAxNi4zem0yOC42LTUuNGM3LjUgNC40IDIEzLjcgOCAXMy45IDg
gIjEgMCA0LjUgMi41IDkuNiA1LjcgNS4yIDMuMSAxMCA41IDYuMiAxMS45IDYuOSAYLjEgMS4xLTi4LjEgMTUuMwMtMjguNS0uMjY0Ny4zLjEgMTUuMwMtN
y4zLS4xLS41LTEwLjUtLjUuMTAuNiA3LjguMSA3LjkuMXy5em0tMTluMyAyMy45Yy4xIDYuNi0uMiA4LjUtMS40IDktLjguMy0xLjUuMi0xLjYtLjItLjQt
My40LS41LTE1LS4xLTE2IC4yLS42IDIEtMS4yIDEuNy0xLjluOSAwIDEuMyAyLjMgMS40IDguNHptNi43LjRjMCA0LjUtLjMgOC4yLS44IDguMi0uNCAwLTE
uMS4xLTEuNS4yLS41LjItLjgtMy43LS45LTguNSAwLTcuNS4yLTguNyAxLjUuOC41IDEuMy4zIDIEuNiAxLjkgMS43IDguNpntNi45IDbLjEgNy4yLS4xID
```

Scan Results

Scan Results page 234

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-ECDSA-AES128-GCM-SHA256	ECDH	ECDSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-ECDSA-AES256-GCM-SHA384	ECDH	ECDSA	AEAD	AESGCM(256)	HIGH
ECDHE-ECDSA-CHACHA20-POLY1305	ECDH	ECDSA	AEAD	CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH



1 SSL Session Caching Information

port 9443/tcp over SSL

QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is disabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 9443/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
------------	----------------

0304	rejected
0399	rejected
0400	rejected
0499	rejected



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 9443/tcp over SSL

QID: 38704
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 02/01/2023
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSh1.2						
4 ECDHE-ECDSA-AES256-GCM-SHA38	ECDHE	x25519	256	yes	128	low
4 ECDHE-ECDSA-AES256-GCM-SHA38	ECDHE	secp384r1	384	yes	192	low
4 ECDHE-ECDSA-AES256-GCM-SHA38	ECDHE	secp256r1	256	yes	128	low
4 ECDHE-ECDSA-AES256-GCM-SHA38	ECDHE	secp521r1	521	yes	260	low
5 ECDHE-ECDSA-CHACHA20-POLY130	ECDHE	x25519	256	yes	128	low
5 ECDHE-ECDSA-CHACHA20-POLY130	ECDHE	secp384r1	384	yes	192	low
5 ECDHE-ECDSA-CHACHA20-POLY130	ECDHE	secp256r1	256	yes	128	low
5 ECDHE-ECDSA-CHACHA20-POLY130	ECDHE	secp521r1	521	yes	260	low
6 ECDHE-ECDSA-AES128-GCM-SHA25	ECDHE	x25519	256	yes	128	low
6 ECDHE-ECDSA-AES128-GCM-SHA25	ECDHE	secp384r1	384	yes	192	low

ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE secp256r1 256	yes	128	low
6	521	yes	260	low
TLSv1.3				



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 9443/tcp over SSL

QID:	38706
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no



1 TLS Secure Renegotiation Extension Support Information

port 9443/tcp over SSL

QID: 42350
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 9443/tcp over SSL

QID: 48340
Category: Information gathering
Associated CVEs: -
Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
Bugtraq ID: -
Service Modified: 04/13/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported

**1 SSL Certificate - Information**

port 9443/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	49:f7:69:a3:f2:19:31:ac:71:83:24:4b:a1:20:1e:6b

(0)Signature Algorithm	ecdsa-with-SHA256
(0)ISSUER NAME	
(0)SUBJECT NAME	
(0)Valid From	Nov 11 07:04:00 2025 GMT
(0)Valid Till	Nov 11 07:04:00 2030 GMT
(0)Public Key Algorithm	id-ecPublicKey
(0)EC Public Key	
(0)	Public-Key: (256 bit)
(0)	pub:
(0)	04:09:84:b1:7e:8d:82:4b:df:5a:e7:d4:90:42:d1:
(0)	50:36:76:54:ae:34:09:18:4b:2e:65:41:69:b0:1e:
(0)	d9:a8:b2:cd:73:47:f5:a0:c9:be:ad:80:83:5c:1c:
(0)	16:11:3e:dd:0b:e7:e1:26:46:f0:39:6b:a0:13:31:
(0)	a4:c5:93:93:3b
(0)	ASN1 OID: prime256v1
(0)	NIST CURVE: P-256
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Alternative Name	critical
(0)	DNS:localhost, IP Address:0.0.0.0
(0)Signature	(72 octets)
(0)	30:46:02:21:00:da:6e:df:15:04:8d:ea:c8:83:bb:b3
(0)	79:22:ee:4c:a8:a4:b9:eb:d3:de:8e:f4:c1:6b:ba:56
(0)	a3:69:a7:89:47:02:21:00:b3:2e:c6:c3:33:c8:b1:4b
(0)	41:ae:66:b7:79:a9:b0:15:41:ec:8d:37:bc:dc:1d:c1
(0)	0b:d0:2d:da:51:3e:b8:6b:01



1 HTTP Public-Key-Pins Security Header Not Detected

port 9443/tcp

QID: 48002
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 07/12/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 9443.

GET / HTTP/1.1

Host: 172.40.123.5:9443

Connection: Keep-Alive



1 HTTP Response Method and Header Information Collected

port 9443/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 9443.

GET / HTTP/1.1

Host: 172.40.123.5:9443

Connection: Keep-Alive

HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Content-Length: 19169
Content-Type: text/html; charset=utf-8
Last-Modified: Tue, 30 Apr 2024 22:47:07 GMT
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Csrf-Token:
X-Xss-Protection: 1; mode=block
Date: Sat, 25 Apr 2026 00:45:14 GMT

1 Referrer-Policy HTTP Security Header Not Detected

port 9443/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 9443 port.
GET / HTTP/1.1

 1 Default Web Page

port 8000/tcp over SSL

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8000
Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Flowise - Build AI Agents, Visually</title>
    <link rel="icon" href="favicon.ico" />
    <!-- Meta Tags-->
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="theme-color" content="#2296f3" />
    <meta name="title" content="Flowise - Build AI Agents, Visually" />
    <meta
      name="description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <link rel="manifest" href="manifest.json" />
    <link rel="apple-touch-icon" href="logo192.png" />
    <meta name="keywords" content="react, material-ui, workflow automation, llm, artificial-intelligence" />
    <meta name="author" content="FlowiseAI" />
    <!-- Open Graph / Facebook -->
    <meta property="og:locale" content="en_US" />
    <meta property="og:type" content="website" />
    <meta property="og:url" content="https://flowiseai.com/" />
    <meta property="og:site_name" content="flowiseai.com" />
    <meta property="og:title" content="Flowise - Build AI Agents, Visually" />
```

```

<meta
  property="og:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<!-- Twitter -->
<meta property="twitter:card" content="summary_large_image" />
<meta property="twitter:url" content="https://twitter.com/FlowiseAI" />
<meta property="twitter:title" content="Flowise - Build AI Agents, Visually" />
<meta
  property="twitter:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<meta name="twitter:creator" content="@FlowiseAI" />

<link rel="preconnect" href="https://fonts.gstatic.com" />
<link
href="https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap"
rel="stylesheet"
/>
<script>
;(function (w, r) {
  w._rwq = r
  w[r] =
    w[r] ||
    function () {
      ;(w[r].q = w[r].q || []).push(arguments)
    }
})(window, 'rewardful')
</script>
<script async src="https://r.wdfl.co/rw.js" data-rewardful="9a3a26"></script>
<script type="module" crossorigin src="/assets/index-C6GKaUTA.js"></script>
<link rel="stylesheet" crossorigin href="/assets/index-9xw-RjBM.css">
</head>

<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root"></div>
<div id="portal"></div>
<script>
  if (global === undefined) {
    var global = window
  }
</script>
</body>
</html>

```

1 Default Web Page (Follow HTTP Redirection)

port 8000/tcp over SSL

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8000
Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Flowise - Build AI Agents, Visually</title>
    <link rel="icon" href="favicon.ico" />
    <!-- Meta Tags -->
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="theme-color" content="#2296f3" />
    <meta name="title" content="Flowise - Build AI Agents, Visually" />
    <meta
      name="description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <link rel="manifest" href="manifest.json" />
    <link rel="apple-touch-icon" href="logo192.png" />
    <meta name="keywords" content="react, material-ui, workflow automation, llm, artificial-intelligence" />
    <meta name="author" content="FlowiseAI" />
    <!-- Open Graph / Facebook -->
    <meta property="og:locale" content="en_US" />
    <meta property="og:type" content="website" />
    <meta property="og:url" content="https://flowiseai.com/" />
    <meta property="og:site_name" content="flowiseai.com" />
    <meta property="og:title" content="Flowise - Build AI Agents, Visually" />
    <meta
      property="og:description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <!-- Twitter -->
    <meta property="twitter:card" content="summary_large_image" />
    <meta property="twitter:url" content="https://twitter.com/FlowiseAI" />
    <meta property="twitter:title" content="Flowise - Build AI Agents, Visually" />
    <meta
      property="twitter:description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <meta name="twitter:creator" content="@FlowiseAI" />

    <link rel="preconnect" href="https://fonts.gstatic.com" />
    <link
      href="https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap"
      rel="stylesheet"
    />
    <script>
      ;(function (w, r) {
        w._rwq = r
        w[r] =
          w[r] ||
          function () {
            ;(w[r].q = w[r].q || []).push(arguments)
          }
      })(window, 'rewardful')
    </script>
    <script async src="https://r.wdfl.co/rw.js" data-rewardful="9a3a26"></script>
    <script type="module" crossorigin src="/assets/index-C6GKaUTA.js"></script>
    <link rel="stylesheet" crossorigin href="/assets/index-9xw-RjBM.css">
  </head>
```

```

<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root"></div>
<div id="portal"></div>
<script>
  if (global === undefined) {
    var global = window
  }
</script>
</body>
</html>

```



1 SSL Server Information Retrieval

port 8000/tcp over SSL

QID: 38116
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 05/24/2016
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM

CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
CAMELLIA128-SHA256	RSA	RSA	SHA256	Camellia(128)	MEDIUM
CAMELLIA256-SHA256	RSA	RSA	SHA256	Camellia(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ARIA128-GCM-SHA256	RSA	RSA	AEAD	ARIAGCM(128)	MEDIUM
ARIA256-GCM-SHA384	RSA	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-ARIA128-GCM-SHA256	ECDH	RSA	AEAD	ARIAGCM(128)	MEDIUM
ECDHE-RSA-ARIA256-GCM-SHA384	ECDH	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-CAMELLIA128-SHA256	ECDH	RSA	SHA256	Camellia(128)	MEDIUM
ECDHE-RSA-CAMELLIA256-SHA384	ECDH	RSA	SHA384	Camellia(256)	HIGH
AES128-CCM	RSA	RSA	AEAD	AESCCM(128)	MEDIUM
AES256-CCM	RSA	RSA	AEAD	AESCCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					



1 SSL Session Caching Information

port 8000/tcp over SSL

QID: 38291
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/19/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 8000/tcp over SSL

QID:

38597

Category:

General remote services

Associated CVEs:

-

Vendor Reference:

-

Bugtraq ID:

-

Service Modified:

07/12/2021

User Modified:

-

Edited:

No

PCI Vuln:

No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1

SSL Certificate will expire within next six months

port 8000/tcp over SSL

QID:

38600

Category:

General remote services

Associated CVEs:

-

Vendor Reference:

-

Bugtraq ID:

-

Service Modified:

11/14/2024

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=172.40.123.5,O=LocalDev,L=Bogota,ST=Cundinamarca,C=CO The certificate will expire within six months: Sep 9 17:01:41 2026 GMT



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 8000/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
AES256-SHA256	RSA		2048	no	110	low
AES128-SHA256	RSA		2048	no	110	low
AES256-CCM	RSA		2048	no	110	low
AES128-CCM	RSA		2048	no	110	low
ARIA256-GCM-SHA384	RSA		2048	no	110	low
ARIA128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA256	RSA		2048	no	110	low
AES256-GCM-SHA384	RSA		2048	no	110	low
AES128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA	RSA		2048	no	110	low
CAMELLIA128-SHA	RSA		2048	no	110	low
AES256-SHA	RSA		2048	no	110	low
AES128-SHA	RSA		2048	no	110	low
CAMELLIA128-SHA256	RSA		2048	no	110	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp256r1	256	yes	128	low

ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 8000/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no



1 Reports if server supports Post Quantum Cryptographic(PQC) Key Exchange Algorithm

port 8000/tcp over SSL

QID: 38994
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

It reports complete list of all host-supported PQC key-exchange algorithms along with full handshake details.
If server hosts any service

over TLS1.3, then a probe is sent to validate if the service supports following PQC key exchange

algorithms.

MLKEM512

MLKEM768

MLKEM1024

X25519MLKEM768

SecP256r1MLKEM768

SecP384r1MLKEM1024

Field

Description

Cipher name
Cipher used

Protocol
TLS

version

Key-exchange
Negotiated PQC KEX

Authentication

Signature algorithm

MAC
Message authentication code

Encryption + key

strength
Encryption mode and key size

NIST security strength
Security strength (NIST

equivalent)

Reference: <https://csrc.nist.gov/groups/ST/post-quantum-crypto/evaluation-criteria.html>

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	STRENGTH
TLS13-AES-256-GCM-SHA384	X25519MLKEM768	RSA-PSS	AEAD	AESGCM(256)	192-bit



1 Reports Signature Algorithm used in Post Quantum Cryptographic(PQC) detection using QID 38994

port 8000/tcp over SSL

QID: 38995
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No

PCI Vuln: No

THREAT:

If server hosts any service over TLS1.3, then a probe is sent to validate if the service supports PQC key exchange algorithms as part of QID38994.

This QID reports Signature Algorithm used by the service for Post Quantum Cryptographic(PQC) SSL handshake using QID 38994.

It

reports server's preferred PQC signature algorithm.

This QID is planned for future deprecation.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Preferred PQC Signature Algorithm: RSA-PSS



1 TLS Secure Renegotiation Extension Support Information

port 8000/tcp over SSL

QID: 42350
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 8000/tcp over SSL

QID: 48340
Category: Information gathering
Associated CVEs: -
Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
Bugtraq ID: -
Service Modified: 04/13/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 8000/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -

Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	21:f2:e0:4f:f6:78:ca:3d:6f:76:84:e9:a0:c0:3d:7c:f1:85:a7:75
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	CO
stateOrProvinceName	Cundinamarca
localityName	Bogota
organizationName	LocalDev
commonName	172.40.123.5
(0)SUBJECT NAME	
countryName	CO
stateOrProvinceName	Cundinamarca
localityName	Bogota
organizationName	LocalDev
commonName	172.40.123.5
(0)Valid From	Sep 9 17:01:41 2025 GMT
(0)Valid Till	Sep 9 17:01:41 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:af:b7:6e:89:13:cd:38:0b:95:02:43:24:77:79:
(0)	0e:c1:21:1a:2f:71:b8:fd:ab:bf:51:a5:9b:04:c7:
(0)	0c:c8:4e:f4:08:de:90:87:1f:92:eb:ff:c6:de:e8:
(0)	d8:e9:23:8c:b8:df:74:51:02:f8:f0:6b:ac:79:b8:
(0)	c9:08:6f:a3:83:d9:08:68:8c:0a:0d:8a:5c:67:50:
(0)	3c:4a:33:43:b9:70:03:e3:a3:30:70:15:c3:e4:0e:
(0)	e0:b7:a4:ce:f5:6c:05:fe:b6:f9:59:e6:b4:38:fa:

(0)	01:3e:40:b5:98:98:3d:ed:f9:9c:ac:6c:79:33:57:
(0)	32:21:8c:04:36:5b:c2:f2:be:53:31:3a:a9:9d:11:
(0)	ea:51:a9:dc:af:6c:c7:8c:22:55:e0:c7:9c:00:58:
(0)	7b:f5:15:c5:13:24:c0:58:57:c2:7f:19:97:2a:e0:
(0)	4c:bd:eb:c4:55:9f:45:a8:aa:eb:2c:45:b7:f0:58:
(0)	54:a4:50:54:0e:15:77:b1:47:46:25:d0:48:9f:b9:
(0)	e3:4b:b8:aa:91:6e:f7:1d:08:41:0d:64:8a:f0:d4:
(0)	04:ee:1e:ca:d4:98:ee:08:b0:e2:e0:28:14:a9:fa:
(0)	85:2c:56:a4:59:97:3d:bc:d8:67:5b:86:c0:64:fb:
(0)	e1:a4:31:44:9b:65:26:c6:0e:d7:79:17:21:f0:fc:
(0)	24:e1
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Subject Key Identifier	0B:D7:FB:F9:0A:82:CA:B6:E3:1D:CE:02:50:7F:87:C2:02:A3:D7:55
(0)X509v3 Authority Key Identifier	keyid:0B:D7:FB:F9:0A:82:CA:B6:E3:1D:CE:02:50:7F:87:C2:02:A3:D7:55
(0)X509v3 Basic Constraints	critical
(0)	CA:TRUE
(0)Signature	(256 octets)
(0)	12:9a:77:1e:ce:9f:7f:50:40:a6:d2:9d:3d:4e:d1:89
(0)	2c:1b:32:6b:f7:fa:ac:33:5f:2c:5b:9a:73:9a:e6:bd
(0)	ee:9a:35:d7:ec:04:d4:fd:af:8c:98:0a:89:c8:4e:8b
(0)	c5:f0:e7:f0:43:03:f4:60:e0:81:e1:20:0d:6b:05:28
(0)	f2:b9:9a:8a:70:44:b7:4d:71:ba:6a:3b:87:d0:b0:b9
(0)	c3:bd:a6:d3:80:89:ef:96:13:19:c9:b8:96:a7:99:a5
(0)	4d:69:3e:84:1d:a6:b3:78:27:13:7b:eb:49:62:6e:4d
(0)	54:1c:59:1e:c9:67:da:c1:92:7b:6d:90:ba:8b:0b:20
(0)	4b:3d:bf:93:38:ca:3b:5c:2d:7d:21:9e:d4:44:28:09
(0)	3e:38:6b:34:b6:cd:49:73:bb:91:7e:50:a5:fb:e0:8a
(0)	e1:0f:95:a7:ce:c0:13:26:6e:c0:04:70:70:45:66:14
(0)	8d:d0:2b:4e:d9:5e:8d:70:45:a7:f8:79:7a:5c:a9:59
(0)	93:5d:9b:5b:1a:a5:af:67:b5:f4:1e:7e:0f:c1:ff:4f
(0)	57:90:2d:9d:5a:e2:ec:02:f6:c5:02:bb:81:53:fb:f4
(0)	7a:a5:3e:01:05:80:af:cc:da:6d:48:f5:13:a4:13:a8
(0)	c5:57:7e:86:8d:a6:55:43:c0:11:68:21:82:a3:01:40

1 Web Server Supports HTTP Request Pipelining

port 8000/tcp over SSL

QID: 86565
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/22/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:8000

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:8000

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:40:35 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 3142
Connection: keep-alive
Vary: Origin
Content-Security-Policy: frame-ancestors
Access-Control-Allow-Credentials: true
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 11 Aug 2025 12:14:01 GMT
ETag: W/"c46-198990d4728"
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Flowise - Build AI Agents, Visually</title>
    <link rel="icon" href="favicon.ico" />
    <!-- Meta Tags-->
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="theme-color" content="#2296f3" />
    <meta name="title" content="Flowise - Build AI Agents, Visually" />
    <meta
      name="description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <link rel="manifest" href="manifest.json" />
    <link rel="apple-touch-icon" href="logo192.png" />
    <meta name="keywords" content="react, material-ui, workflow automation, llm, artificial-intelligence" />
    <meta name="author" content="FlowiseAI" />
    <!-- Open Graph / Facebook -->
    <meta property="og:locale" content="en_US" />
    <meta property="og:type" content="website" />
    <meta property="og:url" content="https://flowiseai.com/" />
    <meta property="og:site_name" content="flowiseai.com" />
    <meta property="og:title" content="Flowise - Build AI Agents, Visually" />
    <meta
      property="og:description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <!-- Twitter -->
    <meta property="twitter:card" content="summary_large_image" />
```

```

<meta property="twitter:url" content="https://twitter.com/FlowiseAI" />
<meta property="twitter:title" content="Flowise - Build AI Agents, Visually" />
<meta
  property="twitter:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<meta name="twitter:creator" content="@FlowiseAI" />

<link rel="preconnect" href="https://fonts.gstatic.com" />
<link
  href="https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap"
  rel="stylesheet"
/>
<script>
  ;(function (w, r) {
    w._rwq = r
    w[r] =
      w[r] ||
      function () {
        ;(w[r].q = w[r].q || []).push(arguments)
      }
  })(window, 'rewardful')
</script>
<script async src="https://r.wdfl.co/rw.js" data-rewardful="9a3a26"></script>
<script type="module" crossorigin src="/assets/index-C6GKaUTA.js"></script>
<link rel="stylesheet" crossorigin href="/assets/index-9xw-RjBM.css">
</head>

<body>
  <noscript>You need to enable JavaScript to run this app.</noscript>
  <div id="root"></div>
  <div id="portal"></div>
  <script>
    if (global === undefined) {
      var global = window
    }
  </script>
</body>
</html>
HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:40:35 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 3142
Connection: keep-alive
Vary: Origin
Content-Security-Policy: frame-ancestors
Access-Control-Allow-Credentials: true
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 11 Aug 2025 12:14:01 GMT
ETag: W/"c46-198990d4728"
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type

<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Flowise - Build AI Agents, Visually</title>
    <link rel="icon" href="favicon.ico" />
    <!-- Meta Tags -->
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="theme-color" content="#2296f3" />
    <meta name="title" content="Flowise - Build AI Agents, Visually" />
    <meta
      name="description"
      content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
    />
    <link rel="manifest" href="manifest.json" />
    <link rel="apple-touch-icon" href="logo192.png" />
    <meta name="keywords" content="react, material-ui, workflow automation, llm, artificial-intelligence" />
    <meta name="author" content="FlowiseAI" />
    <!-- Open Graph / Facebook -->
    <meta property="og:locale" content="en_US" />
    <meta property="og:type" content="website" />

```

```

<meta property="og:url" content="https://flowiseai.com/" />
<meta property="og:site_name" content="flowiseai.com" />
<meta property="og:title" content="Flowise - Build AI Agents, Visually" />
<meta
  property="og:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<!-- Twitter -->
<meta property="twitter:card" content="summary_large_image" />
<meta property="twitter:url" content="https://twitter.com/FlowiseAI" />
<meta property="twitter:title" content="Flowise - Build AI Agents, Visually" />
<meta
  property="twitter:description"
  content="Open source generative AI development platform for building AI agents, LLM orchestration, and more"
/>
<meta name="twitter:creator" content="@FlowiseAI" />

<link rel="preconnect" href="https://fonts.gstatic.com" />
<link
href="https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400;500;600;700&family=Roboto:wght@400;500;700&display=swap"
rel="stylesheet"
/>
<script>
;(function (w, r) {
  w._rwq = r
  w[r] =
    w[r] ||
    function () {
      ;(w[r].q = w[r].q || []).push(arguments)
    }
})(window, 'rewardful')
</script>
<script async src="https://r.wdfl.co/rw.js" data-rewardful="9a3a26"></script>
<script type="module" crossorigin src="/assets/index-C6GKaUTA.js"></script>
<link rel="stylesheet" crossorigin href="/assets/index-9xw-RjBM.css">
</head>

<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root"></div>
<div id="portal"></div>
<script>
  if (global === undefined) {
    var global = window
  }
</script>
</body>
</html>

```



1 Nginx Web Server Detected

port 8089/tcp

QID:	45433
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/15/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Nginx is a web server which can also be used as a reverse proxy, load balancer , mail proxy and HTTP cache.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Nginx Web Server Detected on 8089 over TCP.
Server: nginx/1.29.8

 1 HTTP Public-Key-Pins Security Header Not Detected

port 8089/tcp

QID: 48002
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8089.
GET / HTTP/1.1
Host: 172.40.123.5:8089
Connection: Keep-Alive

 1 HTTP Response Method and Header Information Collected

port 8089/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8089.

GET / HTTP/1.1
Host: 172.40.123.5:8089
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 01:29:04 GMT
Content-Type: text/html
Content-Length: 2706
Last-Modified: Fri, 10 Apr 2026 18:57:21 GMT
Connection: keep-alive
ETag: "69d94811-a92"
Accept-Ranges: bytes

1 Referrer-Policy HTTP Security Header Not Detected

port 8089/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -

Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8089 port.
GET / HTTP/1.1
Host: 172.40.123.5:8089
Connection: Keep-Alive

1 List of Web Directories

port 8089/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/config/	brute force



1 Apache Default Foreign Language File Still on Server

port 8089/tcp

QID: 86743
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/11/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Apache installs foreign language files along with index.html. The files are as follows:

index.html.ca
index.html.de
index.html.dk
index.html.ee

An attacker can get additional information about the Web server from these files.

IMPACT:

Sensitive system information may be disclosed, which can be utilized by an attacker to aid further attacks.

SOLUTION:

Apache recommends to remove these files from the Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /index.html.ru.iso-ru HTTP/1.1
Host: 172.40.123.5:8089
Connection: Keep-Alive



1 Default Web Page

port 8081/tcp

QID: 12230

Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8081
Connection: Keep-Alive

```
<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next="/>/login?next=
</a>. If not, click the link.
```

1 Default Web Page (Follow HTTP Redirection)

port 8081/tcp

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1

Host: 172.40.123.5:8081

Connection: Keep-Alive

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">

  <title>pgAdmin 4</title>

  <meta name="viewport" content="width=device-width, initial-scale=1">

  <!-- To set pgAdmin4 shortcut icon in browser -->
  <link rel="shortcut icon" href="/favicon.ico?ver=91400"/>
  <style>
    .pg-sp-container {
      position: absolute;
      min-width: 100%;
      min-height: 100%;
      background: #090d1199;
      z-index: 1056;
      top: 0;
    }
    .pg-sp-container .pg-sp-content {
      position: absolute;
      width: 100%;
      top: 40%;
    }
    .pg-sp-icon {
      background: url("data:image/svg+xml;charset=UTF-8,%3c?xml version='1.0' encoding='utf-8'?%3e%3csvg version='1.1' id='Layer_1'
xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x='0px' y='0px' viewBox='0 0 38 38' style='enable-background:new 0 0 38 38;'
xml:space='preserve'%3e%3cstyle type='text/css'%3e .st0%7bfill:none;stroke:%23ebeeef3;stroke-width:2;%7d .st1%7bfill:none;stroke:%23326690;stroke-width:2;%7d
%3c/style%3e%3cg%3e%3cg transform='translate(1 1)'%3e%3ccircle class='st0' cx='18' cy='18' r='18'/%3e%3cpath class='st1' d='M36,18c0-9.9-8.1-18-18
'%3e%3canimateTransform accumulate='none' additive='replace' attributeName='transform' calcMode='linear' dur='0.7s' fill='remove' from='0 18 18'
repeatCount='indefinite' restart='always' to='360 18 18' type='rotate'%3e%3c/animateTransform%3e%3c/path%3e%3c/g%3e%3c/g%3e%3c/svg%3e") center center
no-repeat;
      height: 75px;
      width: 100%;
      text-align: center;
    }
    .pg-sp-text {
      font-size: 20px;
      text-align: center;
      color: #fff;
    }
  </style>

  <!-- Base template stylesheets -->
  <link type="text/css" rel="stylesheet" href="/static/js/generated/style.css?ver=91400"/>

  <!--View specified stylesheets-->

  <script type="application/javascript">
```

```

/* This is used to change publicPath of webpack at runtime */
window.resourceBasePath = "/static/js/generated/";
</script>
<script type="application/javascript"
  src="/static/vendor/require/require.min.js?ver=91400"></script>
<!-- Base template scripts -->
<script type="application/javascript">
  require.config({
    baseUrl: "",
    urlArgs: 'ver=91400',
    waitSeconds: 0,
    shim: {},
    paths: {
      sources: "/static/js",
      datagrid: "/static/js/generated/datagrid",
      sqleditor: "/static/js/generated/sqleditor",
      'pgadmin.browser.utils': "/browser/" + "js/utils",
      'pgadmin.browser.endpoints': "/browser/" + "js/endpoints",
      'pgadmin.browser.messages': "/browser/" + "js/messages",
      'pgadmin.server.supported_servers': "/browser/" + "server/supported_servers",
      'pgadmin.user_management.current_user': "/user_management/" + "current_user",
      'translations': "/tools/" + "translations",
      'security.pages': "/static/js/generated/security.pages"
    }
  });

</script>
<script type="application/javascript" src="/static/js/generated/vendor.react.js?ver=91400" ></script>
<script type="application/javascript" src="/static/js/generated/vendor.main.js?ver=91400" ></script>
<script type="application/javascript" src="/static/js/generated/vendor.others.js?ver=91400" ></script>
<script type="application/javascript" src="/static/js/generated/vendor.sqleditor.js?ver=91400"></script>
<script type="application/javascript" src="/static/js/generated/pgadmin_commons.js?ver=91400" ></script>

</head>
<body>
<style>
body {
  -webkit-user-select: none;
  -moz-user-select: none;
  -ms-user-select: none;
  user-select: none;
  font-size: 0.875rem;
  height: 100vh;
  overflow: hidden;
  margin: 0;
  font-family: "Roboto", "Helvetica Neue", -apple-system, BlinkMacSystemFont, "Segoe UI", Arial, sans-serif, "Apple Color Emoji", "Segoe UI Emoji", "Segoe
  UI Symbol", "Noto Color Emoji";
}
</style>
<!--[if lt IE 7]>
<p class="browsehappyy">You are using an <strong>outdated</strong> browser. Please <a href="http://browsehappy.com/">upgrade
  your browser</a> to improve your experience.</p>
<![endif]>-->

<style>
  #root:not(:empty) + .pg-sp-container {
    display: none;
  }
</style>
<div id="root" style="height: 100%"></div>
<div class="pg-sp-container">
  <div class="pg-sp-content">
    <div class="pg-sp-icon"></div>
  </div>
</div>
<script type="application/javascript">
  try {
    require(
      ['security.pages'],
      function() {
        window.renderSecurityPage('login_user', { 'authSources': ['internal'], 'authSourcesEnum': { 'KERBEROS': 'kerberos', 'OAUTH2': 'oauth2' },
        'csrfToken': '1jViNjM2ZTlZNTNmMmNjNjQ1NzFhMDcwN2ZjNzQ5OTY3ZjU0NDYzNjgi.aewbHQ.qRP_PiUMLvNJB4j0y3ODbDZybJE', 'forgotPassUrl': '/browser/reset_password',
        'langOptions': [{ 'label': 'English', 'value': 'en' }, { 'label': 'Chinese (Simplified)', 'value': 'zh_Hans_CN' }, { 'label': 'Chinese (Traditional)', 'value':
        'zh_Hant_TW' }, { 'label': 'Czech', 'value': 'cs' }, { 'label': 'French', 'value': 'fr' }, { 'label': 'German', 'value': 'de' }, { 'label': 'Indonesian', 'value':
        'id' }, { 'label': 'Italian', 'value': 'it' }, { 'label': 'Japanese', 'value': 'ja' }, { 'label': 'Korean', 'value': 'ko' }, { 'label': 'Polish', 'value': 'pl' },
        { 'label': 'Portuguese (Brazilian)', 'value': 'pt_BR' }, { 'label': 'Russian', 'value': 'ru' }, { 'label': 'Spanish', 'value': 'es' }, { 'label': 'Swedish',
        'value': 'sv' } ], 'loginBanner': '', 'loginUrl': '/authenticate/login', 'oauth2Config': { 'OAUTH2_BUTTON_COLOR': null, 'OAUTH2_DISPLAY_NAME': '\u003cOauth2
        Display Name\u003e', 'OAUTH2_ICON': null, 'OAUTH2_NAME': null }, 'userLanguage': 'en' },

```

```
        {"messages": []});
    }, function() {
        console.log(arguments);
    }
);
} catch (err) {
    console.log(err);
}
</script>

</body>
</html>
```

1 HTTP Methods Returned by OPTIONS Request

port 8081/tcp

QID: 45056
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/16/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Allow: OPTIONS, HEAD, GET

1 HTTP Response Method and Header Information Collected

port 8081/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8081.

GET / HTTP/1.1
Host: 172.40.123.5:8081
Connection: Keep-Alive

HTTP/1.1 302 FOUND
Server: unicorn
Date: Sat, 25 Apr 2026 01:37:38 GMT
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Length: 213
Location: /login?next=/
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src ws: http: data: blob: 'unsafe-inline' 'unsafe-eval';
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cross-Origin-Opener-Policy: same-origin
Set-Cookie: pga4_session=f2f46478-3ca3-40a0-a7b9-a5ea9f281ba0!7UsJho6ncJtakzqerKeBxwSXpZGs4yeaomnpYctYl5U=; Expires=Sun, 26 Apr 2026 01:37:38 GMT; HttpOnly; Path=/; SameSite=Lax



1 Referrer-Policy HTTP Security Header Not Detected

port 8081/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8081 port.
GET / HTTP/1.1
Host: 172.40.123.5:8081
Connection: Keep-Alive



1 List of Web Directories

port 8081/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/browser/	brute force
/about/	brute force
/#/	brute force
/cloud/	brute force
/login	brute force
/static/	web page
/static/js/	web page
/static/js/generated/	web page

**1 Default Web Page**

port 9000/tcp

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:9000
Connection: Keep-Alive

```
<!doctype html>
<html lang="en">
<head>
  <script type="module" crossorigin src="/js/polyfills-jkv3S6Ta.js"></script>

  <meta http-equiv="content-type" content="text/html; charset=UTF-8" charset="UTF-8" />
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <link rel="apple-touch-icon" href="/apple-touch-icon.png" />
  <link rel="icon" type="image/x-icon" href="/favicon.ico" />
```

```

<meta name="application-name" content="SonarQube" />
<meta name="msapplication-TileColor" content="#FFFFFF" />
<meta name="msapplication-TileImage" content="/mstile-512x512.png" />
<title>SonarQube</title>
<script>
  window.__assetsPath = function (filename) {
    return '/' + filename;
  };
</script>
<script type="module" crossorigin src="/js/main-XxImVjZg.js"></script>
<link rel="modulepreload" crossorigin href="/js/vendor-UHIUeQ8n.js">
<link rel="modulepreload" crossorigin href="/js/echoes-CyKugzeJ.js">
<link rel="modulepreload" crossorigin href="/js/lodash-Bs6y92dJ.js">
<link rel="modulepreload" crossorigin href="/js/highlightjs-CFvgWmRf.js">
<link rel="modulepreload" crossorigin href="/js/date-fns-BK34w00l.js">
<link rel="stylesheet" crossorigin href="/css/echoes-B01CWL15.css">
<link rel="stylesheet" crossorigin href="/css/main-DrqbZo7l.css">
</head>

<body>
  <div
    id="content"
    data-base-url=""
    data-server-status="UP"
    data-instance="SonarQube"
    data-official="true"
  >
    <div class="global-loading">
      <i class="global-loading-spinner"></i>
      <span aria-live="polite" class="global-loading-text">Loading...</span>
    </div>
  </div>
</body>
</html>

```



1 Default Web Page (Follow HTTP Redirection)

port 9000/tcp

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:9000
Connection: Keep-Alive

```
<!doctype html>
<html lang="en">
  <head>
    <script type="module" crossorigin src="/js/polyfills-jkv3S6Ta.js"></script>

    <meta http-equiv="content-type" content="text/html; charset=UTF-8" charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <link rel="apple-touch-icon" href="/apple-touch-icon.png" />
    <link rel="icon" type="image/x-icon" href="/favicon.ico" />
    <meta name="application-name" content="SonarQube" />
    <meta name="msapplication-TileColor" content="#FFFFFF" />
    <meta name="msapplication-TileImage" content="/mstile-512x512.png" />
    <title>SonarQube</title>
    <script>
      window.__assetsPath = function (filename) {
        return '/' + filename;
      };
    </script>
    <script type="module" crossorigin src="/js/main-XxImVjZg.js"></script>
    <link rel="modulepreload" crossorigin href="/js/vendor-UHIUeQ8n.js">
    <link rel="modulepreload" crossorigin href="/js/echoes-CyKugzeJ.js">
    <link rel="modulepreload" crossorigin href="/js/lodash-Bs6y92dJ.js">
    <link rel="modulepreload" crossorigin href="/js/highlightjs-CFvgWmRf.js">
    <link rel="modulepreload" crossorigin href="/js/date-fns-BK34w00l.js">
    <link rel="stylesheet" crossorigin href="/css/echoes-B01CWL15.css">
    <link rel="stylesheet" crossorigin href="/css/main-DrqbZo7l.css">
  </head>

  <body>
    <div
      id="content"
      data-base-url=""
      data-server-status="UP"
      data-instance="SonarQube"
      data-official="true"
    >
      <div class="global-loading">
        <i class="global-loading-spinner"></i>
        <span aria-live="polite" class="global-loading-text">Loading...</span>
      </div>
    </div>
  </body>
</html>
```

1 HTTP Methods Returned by OPTIONS Request

port 9000/tcp

QID:	45056
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS



1 HTTP Response Method and Header Information Collected

port 9000/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 9000.

GET / HTTP/1.1
Host: 172.40.123.5:9000
Connection: Keep-Alive

HTTP/1.1 200
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 0
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; base-uri 'none'; connect-src 'self' http: https:; font-src 'self' data:; frame-src; img-src * data: blob:; object-src 'none'; script-src 'self' 'sha256-D1jaqcDDM2TM2STrzE42NNqyKR9PlptcHDe6tyaBcuM='; style-src 'self' 'unsafe-inline'; worker-src 'self'
Cache-Control: no-cache, no-store, must-revalidate
vary: accept-encoding
Content-Type: text/html; charset=utf-8
Content-Length: 1698
Date: Sat, 25 Apr 2026 01:42:10 GMT
Keep-Alive: timeout=60
Connection: keep-alive



1 Referrer-Policy HTTP Security Header Not Detected

port 9000/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 9000 port.
GET / HTTP/1.1
Host: 172.40.123.5:9000
Connection: Keep-Alive



1 SonarSource SonarQube Detected

port 9000/tcp

QID: 48163
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/06/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SonarQube is an automatic code review tool to detect bugs, vulnerabilities, and code smells in your code. It can integrate with your existing workflow to enable continuous code inspection across your project branches and pull requests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SonarSource SonarQube Version detected on port : 9000.
"version": "26.4.0.121862",



1 Web Server Supports HTTP Request Pipelining

port 9000/tcp

QID: 86565
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/22/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:9000

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:9000

HTTP/1.1 200
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 0
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; base-uri 'none'; connect-src 'self' http: https:; font-src 'self' data:; frame-src; img-src * data: blob:; object-src 'none'; script-src 'self' 'sha256-D1jaqcDDM2TM2STrzE42NNqyKR9PlptcHDe6tyaBcuM='; style-src 'self' 'unsafe-inline'; worker-src 'self'
Cache-Control: no-cache, no-store, must-revalidate
vary: accept-encoding
Content-Type: text/html; charset=utf-8
Content-Length: 1698
Date: Sat, 25 Apr 2026 02:41:35 GMT

```
<!doctype html>
<html lang="en">
<head>
  <script type="module" crossorigin src="/js/polyfills-jkv3S6Ta.js"></script>

  <meta http-equiv="content-type" content="text/html; charset=UTF-8" charset="UTF-8" />
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <link rel="apple-touch-icon" href="/apple-touch-icon.png" />
  <link rel="icon" type="image/x-icon" href="/favicon.ico" />
  <meta name="application-name" content="SonarQube" />
  <meta name="msapplication-TileColor" content="#FFFFFF" />
  <meta name="msapplication-TileImage" content="/mstile-512x512.png" />
  <title>SonarQube</title>
  <script>
    window.__assetsPath = function (filename) {
      return '/' + filename;
    };
  </script>
  <script type="module" crossorigin src="/js/main-XxlmVjZg.js"></script>
  <link rel="modulepreload" crossorigin href="/js/vendor-UHlUeQ8n.js">
  <link rel="modulepreload" crossorigin href="/js/echoes-CyKugzeJ.js">
  <link rel="modulepreload" crossorigin href="/js/lodash-Bs6y92dJ.js">
  <link rel="modulepreload" crossorigin href="/js/highlightjs-CFvgWmRf.js">
  <link rel="modulepreload" crossorigin href="/js/datefmts-BK34w00l.js">
  <link rel="stylesheet" crossorigin href="/css/echoes-B01CWL15.css">
```

```

<link rel="stylesheet" crossorigin href="/css/main-DrqbZo7l.css">
</head>

<body>
<div
  id="content"
  data-base-url=""
  data-server-status="UP"
  data-instance="SonarQube"
  data-official="true"
>
  <div class="global-loading">
    <i class="global-loading-spinner"></i>
    <span aria-live="polite" class="global-loading-text">Loading...</span>
  </div>
</div>
</body>
</html>
HTTP/1.1 200
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 0
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; base-uri 'none'; connect-src 'self' http: https:; font-src 'self' data:; frame-src; img-src * data: blob:;
object-src 'none'; script-src 'self' 'sha256-D1jaqcDDM2TM2STrzE42NNqyKR9PlptcHDe6tyaBcuM='; style-src 'self' 'unsafe-inline'; worker-src 'self'
Cache-Control: no-cache, no-store, must-revalidate
vary: accept-encoding
Content-Type: text/html; charset=utf-8
Content-Length: 1698
Date: Sat, 25 Apr 2026 02:41:35 GMT

<!doctype html>
<html lang="en">
<head>
  <script type="module" crossorigin src="/js/polyfills-jkv3S6Ta.js"></script>

  <meta http-equiv="content-type" content="text/html; charset=UTF-8" charset="UTF-8" />
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <link rel="apple-touch-icon" href="/apple-touch-icon.png" />
  <link rel="icon" type="image/x-icon" href="/favicon.ico" />
  <meta name="application-name" content="SonarQube" />
  <meta name="msapplication-TileColor" content="#FFFFFF" />
  <meta name="msapplication-TileImage" content="/mstile-512x512.png" />
  <title>SonarQube</title>
  <script>
    window.__assetsPath = function (filename) {
      return '/' + filename;
    };
  </script>
  <script type="module" crossorigin src="/js/main-XxlmVjZg.js"></script>
  <link rel="modulepreload" crossorigin href="/js/vendor-UHlUeQ8n.js">
  <link rel="modulepreload" crossorigin href="/js/echoes-CyKugzeJ.js">
  <link rel="modulepreload" crossorigin href="/js/lodash-Bs6y92dJ.js">
  <link rel="modulepreload" crossorigin href="/js/highlightjs-CFvgWmRf.js">
  <link rel="modulepreload" crossorigin href="/js/datefmt-BK34w00l.js">
  <link rel="stylesheet" crossorigin href="/css/echoes-B01CWL15.css">
  <link rel="stylesheet" crossorigin href="/css/main-DrqbZo7l.css">
</head>

<body>
<div
  id="content"
  data-base-url=""
  data-server-status="UP"
  data-instance="SonarQube"
  data-official="true"
>
  <div class="global-loading">
    <i class="global-loading-spinner"></i>
    <span aria-live="polite" class="global-loading-text">Loading...</span>
  </div>
</div>
</body>
</html>

```

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/js/	web page
/css/	web page
/api/	brute force
/api	brute force

1 Apache Default Foreign Language File Still on Server

port 9000/tcp

QID: 86743
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/11/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Apache installs foreign language files along with index.html. The files are as follows:

index.html.ca
index.html.de
index.html.dk
index.html.ee

An attacker can get additional information about the Web server from these files.

IMPACT:

Sensitive system information may be disclosed, which can be utilized by an attacker to aid further attacks.

SOLUTION:

Apache recommends to remove these files from the Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /index.html.ru.iso-ru HTTP/1.1
Host: 172.40.123.5:9000
Connection: Keep-Alive



1 Default Web Page

port 8095/tcp

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8095
Connection: Keep-Alive

HTTP/1.1 404 Not Found
content-type: text/html
Date: Sat, 25 Apr 2026 01:49:18 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Transfer-Encoding: chunked

<!DOCTYPE HTML>

```

<html lang="en">
<head>
  <meta charset="utf-8">
  <title>JupyterHub</title>
  <meta http-equiv="X-UA-Compatible" content="chrome=1">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">

  <link rel="stylesheet"

href="/jupyterhub/hub/static/css/style.min.css?v=1169d53348a10b2020fa67f02516a65c955f1483603703fdb5d65653c099dc66f2a52246ae0856c6f1ebcc5e1c5f527a3fa9210d12e6
d8ec77e0e095d9b2c734"
  type="text/css" />

  <link rel="icon"
href="/jupyterhub/hub/static/favicon.ico?v=fde5757cd3892b979919d3b1faa88a410f28829feb5ba22b6cf069f2c6c98675fcee90f932e49b510e74d65c681d5846b943e7f7cc1b41867
422f0481085c1f" type="image/x-icon">

  <script
src="/jupyterhub/hub/static/components/bootstrap/dist/js/bootstrap.bundle.min.js?v=1ef3a326b7703690db9062481b664da83955a8ca3beea6ece0c7b871a8741e80eb7e1adb03
ef12065667d4aaef010c3b7082cb3c526f770220a61cd098c9be3f"
  type="text/javascript"
  charset="utf-8"></script>
  <script
src="/jupyterhub/hub/static/components/requirejs/require.js?v=1ff44af658602d913b22fca97c78f98945f47e76dacf9800f32f35350f05e9acda6dc710b8501579076f3980de02f02
c97f5994ce1a9864c21865a42262d79ec"
  type="text/javascript"
  charset="utf-8"></script>
  <script
src="/jupyterhub/hub/static/components/jquery/dist/jquery.min.js?v=bf6089ed4698cb8270a8b0c8ad9508ff886a7a842278e98064d5c1790ca3a36d5d69d9f047ef196882554fc104
da2c88eb5395f1ee8cf0f3f6ff8869408350fe"
  type="text/javascript"
  charset="utf-8"></script>
  <script
src="/jupyterhub/hub/static/js/darkmode.js?v=2fd9a7d11ad78df9351fed40ab35eab52e1e6a3d516f188b652120e6faf57b8e387a30aae8f52a6fb51563d06d04545c7005da0b77a98c21
b0bd28f6d1cdfa11"
  type="text/javascript"
  charset="utf-8"></script>

<script type="text/javascript">
  require.config({

    urlArgs: "v=20260413153118",

    baseUrl: '/jupyterhub/hub/static/js',
    paths: {
      components: '../components',
      jquery: '../components/jquery/dist/jquery.min',
      moment: '../components/moment/moment',
    },
  });

  window.jhdata = {
    base_url: "/jupyterhub/hub/",
    prefix: "/jupyterhub/",

    admin_access: false,

    options_form: false,

    xsrf_token:
"MnwxOjB8MTA6MTc3NzA4MTc1OHw1OI94c3JmDY4OIRtOXVaVHAzYmtZM2FXbFNjMUZaTkV4TGNVOW5aMjUzUlhsNk4xTXdVRlpXTmxWc05uaHliM1ZRZG1wdlEwUjNQUT09fDI2YWNmYTQyNTA3MzYxOGUx
MTNlNDU0MmNiOGMzMjEzMTYyQ5MmM2OGM2OTVhZTM3OTMxZGMxZTc",
  };
</script>

  <meta name="description" content="JupyterHub">
  <meta name="keywords" content="Jupyter, JupyterHub">

</head>
<body>

```

```

<noscript>
  <div id='noscript'>
    JupyterHub requires JavaScript.
    <br>
    Please enable it to proceed.
  </div>
</noscript>

<nav class="navbar navbar-expand-sm bg-body-tertiary mb-4">
  <div class="container-fluid">

    <span id="jupyterhub-logo" class="navbar-brand">
      <a href="/jupyterhub/hub/home">
        
      <ul class="navbar-nav me-auto mb-0">

        </ul>
        <ul class="nav navbar-nav me-2">

          <li class="nav-item">

            <button class="btn btn-sm"
              id="dark-theme-toggle"
              aria-label="Toggle dark mode"
              title="Toggle dark mode">
              <i aria-hidden="true" class="fa fa-circle-half-stroke"></i>
            </button>

          </li>
          <li class="nav-item">

            </li>

        </ul>
      </div>

    </div>
  </nav>

```

```

<div class="error">

```

```

  <h1>404 : Not Found</h1>

```

```

  <p>Jupyter has lots of moons, but this is not one...</p>

```

```

</div>

```

```

<div class="modal fade"
  id="error-dialog"
  tabindex="-1"
  role="dialog"
  aria-labelledby="error-label"
  aria-hidden="true">
  <div class="modal-dialog">
    <div class="modal-content">
      <div class="modal-header">
        <h2 class="modal-title" id="error-label">Error</h2>
        <button type="button"

```

```

        class="btn-close"
        data-bs-dismiss="modal"
        aria-label="Close"></button>
</div>
<div class="modal-body">
<div class="ajax-error alert-danger">The error</div>
</div>
<div class="modal-footer">
<button type="button"
        class="btn btn-primary"
        data-bs-dismiss="modal"
        data-dismiss="modal">OK</button>
</div>
</div>
</div>
</div>

<script type="text/javascript">
function _remove_redirects_from_url() {
    if (window.location.search.length <= 1) {
        return;
    }
    var search_parameters = window.location.search.slice(1).split('&');
    for (var i = 0; i < search_parameters.length; i++) {
        if (search_parameters[i].split('=')[0] === 'redirects') {
            // remove redirects from search parameters
            search_parameters.splice(i, 1);
            var new_search = "";
            if (search_parameters.length) {
                new_search = '?' + search_parameters.join('&');
            }
            var new_url = window.location.origin +
                window.location.pathname +
                new_search +
                window.location.hash;
            window.history.replaceState({}, "", new_url);
            return;
        }
    }
}

_remove_redirects_from_url();
</script>

</body>
</html>-CR-

```



1 Default Web Page (Follow HTTP Redirection)

port 8095/tcp

QID: 13910
 Category: CGI
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 11/05/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8095
Connection: Keep-Alive

HTTP/1.1 404 Not Found
content-type: text/html
Date: Sat, 25 Apr 2026 01:51:01 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Transfer-Encoding: chunked

```
<!DOCTYPE HTML>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>JupyterHub</title>
    <meta http-equiv="X-UA-Compatible" content="chrome=1">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

```
  <link rel="stylesheet"
```

```
    href="/jupyterhub/hub/static/css/style.min.css?v=1169d53348a10b2020fa67f02516a65c955f1483603703fdb5d65653c099dc66f2a52246ae0856c6f1ebcc5e1c5f527a3fa9210d12e6d8ec77e0e095d9b2c734"
    type="text/css" />
```

```
  <link rel="icon"
```

```
    href="/jupyterhub/hub/static/favicon.ico?v=fde5757cd3892b979919d3b1faa88a410f28829feb5ba22b6cf069f2c6c98675fceef90f932e49b510e74d65c681d5846b943e7f7cc1b41867422f0481085c1f" type="image/x-icon">
```

```
  <script
```

```
    src="/jupyterhub/hub/static/components/bootstrap/dist/js/bootstrap.bundle.min.js?v=1ef3a326b7703690db9062481b664da83955a8ca3beea6ece0c7b871a8741e80eb7e1adb03ef12065667d4aaef010c3b7082cb3c526f770220a61cd098c9be3f"
```

```
    type="text/javascript"
    charset="utf-8"></script>
```

```
  <script
```

```
    src="/jupyterhub/hub/static/components/requirejs/require.js?v=1ff44af658602d913b22fca97c78f98945f47e76dacf9800f32f35350f05e9acda6dc710b8501579076f3980de02f02c97f5994ce1a9864c21865a42262d79ec"
```

```
    type="text/javascript"
    charset="utf-8"></script>
```

```
  <script
```

```
    src="/jupyterhub/hub/static/components/jquery/dist/jquery.min.js?v=bf6089ed4698cb8270a8b0c8ad9508ff886a7a842278e98064d5c1790ca3a36d5d69d9f047ef196882554fc104da2c88eb5395f1ee8cf0f3f6ff8869408350fe"
```

```
    type="text/javascript"
    charset="utf-8"></script>
```

```
  <script
```

```
    src="/jupyterhub/hub/static/js/darkmode.js?v=2fd9a7d11ad78df9351fed40ab35eab52e1e6a3d516f188b652120e6faf57b8e387a30aae8f52a6fb51563d06d04545c7005da0b77a98c21b0bd28f6d1cdfa11"
```

```
    type="text/javascript"
    charset="utf-8"></script>
```

```
<script type="text/javascript">
  require.config({
```

```
    urlArgs: "v=20260413153118",
```

```

    baseUrl: '/jupyterhub/hub/static/js',
    paths: {
      components: '../components',
      jquery: '../components/jquery/dist/jquery.min',
      moment: "../components/moment/moment",
    },
  });

window.jhdata = {
  base_url: "/jupyterhub/hub/",
  prefix: "/jupyterhub/",

  admin_access: false,

  options_form: false,

  xsrf_token:
    "MnwXOjB8MTA6MTc3NzA4MTg2MXw1OI94c3JmfDY4OIRtOXVaVHAzYmtZM2FXbFmjMUZaTKv4TGNVOW5aMjUzUlhsNk4xTXdVRlpXTmxWc05uaHliM1ZRZG1wdlEwUjNQUt09fDY2OWM2OGJhY2JjMGQwZDFhMzk5YmFkZGNINjRIOTJhZjVkJExNWl5YjAyYWVYNDM4MTBjNTUyNGJIN2I2Mjk",
  };
</script>

<meta name="description" content="JupyterHub">
<meta name="keywords" content="Jupyter, JupyterHub">

</head>
<body>
<noscript>
  <div id="noscript">
    JupyterHub requires JavaScript.
    <br>
    Please enable it to proceed.
  </div>
</noscript>

<nav class="navbar navbar-expand-sm bg-body-tertiary mb-4">
  <div class="container-fluid">

    <span id="jupyterhub-logo" class="navbar-brand">
      <a href="/jupyterhub/hub/home">
        
      </a>
    </span>

    <div class="collapse navbar-collapse" id="thenavbar">
      <ul class="navbar-nav me-auto mb-0">

        <ul>
          <li class="nav navbar-nav me-2">

            <li class="nav-item">

              <button class="btn btn-sm"
                id="dark-theme-toggle"
                aria-label="Toggle dark mode"
                title="Toggle dark mode">
                <i aria-hidden="true" class="fa fa-circle-half-stroke"></i>
              </button>

            </li>
            <li class="nav-item">

          </li>

        </ul>
      </div>
    </div>
  </div>

```

```
</div>
</nav>
```

```
<div class="error">
```

```
<h1>404 : Not Found</h1>
```

```
<p>Jupyter has lots of moons, but this is not one...</p>
```

```
</div>
```

```
<div class="modal fade"
  id="error-dialog"
  tabindex="-1"
  role="dialog"
  aria-labelledby="error-label"
  aria-hidden="true">
<div class="modal-dialog">
<div class="modal-content">
<div class="modal-header">
  <h2 class="modal-title" id="error-label">Error</h2>
  <button type="button"
    class="btn-close"
    data-bs-dismiss="modal"
    aria-label="Close"></button>
</div>
<div class="modal-body">
<div class="ajax-error alert-danger">The error</div>
</div>
<div class="modal-footer">
  <button type="button"
    class="btn btn-primary"
    data-bs-dismiss="modal"
    data-dismiss="modal">OK</button>
</div>
</div>
</div>
</div>
```

```
<script type="text/javascript">
function _remove_redirects_from_url() {
  if (window.location.search.length <= 1) {
    return;
  }
  var search_parameters = window.location.search.slice(1).split('&');
  for (var i = 0; i < search_parameters.length; i++) {
    if (search_parameters[i].split('=')[0] === 'redirects') {
      // remove redirects from search parameters
      search_parameters.splice(i, 1);
      var new_search = "";
      if (search_parameters.length) {
        new_search = '?' + search_parameters.join('&');
      }
      var new_url = window.location.origin +
        window.location.pathname +
        new_search +
        window.location.hash;
      window.history.replaceState({}, "", new_url);
      return;
    }
  }
}
_remove_redirects_from_url();
</script>
```

</body>
</html>-CR-

1 HTTP Response Method and Header Information Collected

port 8095/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8095.

GET / HTTP/1.1
Host: 172.40.123.5:8095
Connection: Keep-Alive

HTTP/1.1 404 Not Found
content-type: text/html
Date: Sat, 25 Apr 2026 01:49:18 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Transfer-Encoding: chunked

1 Web Server Supports HTTP Request Pipelining

port 8095/tcp

QID: 86565
Category: Web server
Associated CVEs: -
Vendor Reference: -

Bugtraq ID: -
Service Modified: 02/22/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:8095

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:8095

1 List of Web Directories

port 8095/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/jupyterhub/	web page
/jupyterhub/hub/	web page



1 HTTP Response Method and Header Information Collected

port 8088/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8088.

GET / HTTP/1.1
Host: 172.40.123.5:8088
Connection: Keep-Alive

HTTP/1.1 404 Not Found
date: Sat, 25 Apr 2026 02:10:06 GMT
server: uvicorn
content-length: 22
content-type: application/json



1 List of Web Directories

port 8088/tcp

QID: 86672
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/api/	brute force



1 Default Web Page

port 5002/tcp

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:5002
Connection: Keep-Alive

```
<!doctype html>
<html style="height: 100%" dir="ltr" lang="en">
<head>
  <meta charset="UTF-8" />
  <base href="/" />
  <link rel="icon" type="image/png" href="/static/pin_32.png" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>Airflow</title>
  <script type="module" crossorigin src="/static/assets/index-DMFz1oOG.js"></script>

</head>
<body style="height: 100%">
  <div id="root" style="height: 100%"></div>
</body>
</html>
```

	1	Default Web Page (Follow HTTP Redirection)	port 5002/tcp
QID:	13910		
Category:	CGI		
Associated CVEs:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	11/05/2020		
User Modified:	-		
Edited:	No		
PCI Vuln:	No		

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:5002
Connection: Keep-Alive

```

<!doctype html>
<html style="height: 100%" dir="ltr" lang="en">
<head>
  <meta charset="UTF-8" />
  <base href="/" />
  <link rel="icon" type="image/png" href="/static/pin_32.png" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>Airflow</title>
  <script type="module" crossorigin src="/static/assets/index-DMFz1oOG.js"></script>

</head>
<body style="height: 100%">
  <div id="root" style="height: 100%"></div>
</body>
</html>

```



1 HTTP Response Method and Header Information Collected

port 5002/tcp

QID: 48118
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 07/20/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5002.

GET / HTTP/1.1
 Host: 172.40.123.5:5002
 Connection: Keep-Alive

HTTP/1.1 200 OK
 date: Sat, 25 Apr 2026 02:17:26 GMT

server: uvicorn
content-length: 493
content-type: text/html; charset=utf-8
vary: Accept-Encoding

1 Referrer-Policy HTTP Security Header Not Detected

port 5002/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 5002 port.
GET / HTTP/1.1
Host: 172.40.123.5:5002
Connection: Keep-Alive

1 List of Web Directories

port 5002/tcp

QID: 86672
Category: Web server

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/auth/	brute force
/auth/login/	brute force
/auth/	web page
/auth/static/	web page
/auth/static/appbuilder/	web page
/auth/static/appbuilder/css/	web page
/auth/static/appbuilder/css/fontawesome/	web page
/auth/static/appbuilder/css/select2/	web page
/auth/static/dist/	web page
/auth/static/appbuilder/js/	web page



1 Apache Default Foreign Language File Still on Server

port 5002/tcp

QID: 86743
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/11/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Apache installs foreign language files along with index.html. The files are as follows:

index.html.ca
index.html.de
index.html.dk
index.html.ee

An attacker can get additional information about the Web server from these files.

IMPACT:

Sensitive system information may be disclosed, which can be utilized by an attacker to aid further attacks.

SOLUTION:

Apache recommends to remove these files from the Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /index.html.ru.iso-ru HTTP/1.1
Host: 172.40.123.5:5002
Connection: Keep-Alive

 1 HTTP Public-Key-Pins Security Header Not Detected

port 8091/tcp

QID: 48002
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8091.
GET / HTTP/1.1
Host: 172.40.123.5:8091
Connection: Keep-Alive



1 HTTP Response Method and Header Information Collected

port 8091/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8091.

GET / HTTP/1.1
Host: 172.40.123.5:8091
Connection: Keep-Alive

HTTP/1.1 200 OK
date: Sat, 25 Apr 2026 02:24:07 GMT
server: uvicorn
content-length: 50
content-type: application/json



1 Referrer-Policy HTTP Security Header Not Detected

port 8091/tcp

QID: 48131
Category: Information gathering
Associated CVEs: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Service Modified: 01/18/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8091 port.
GET / HTTP/1.1
Host: 172.40.123.5:8091
Connection: Keep-Alive



1 List of Web Directories

port 8091/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/#/	brute force



1 Default Web Page

port 9090/tcp over SSL

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:9090
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 01:03:29 GMT
Content-Type: text/html
Content-Length: 471
Last-Modified: Fri, 24 Apr 2026 20:28:05 GMT
Connection: keep-alive
ETag: "69ebd255-1d7"
Accept-Ranges: bytes

<!doctype html>

```

<html lang="en">
<head>
  <meta charset="UTF-8" />
  <link rel="icon" type="image/svg+xml" href="/favicon.svg" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>validacion-documentos</title>
  <script type="module" crossorigin src="/assets/index-DdqSzP-5.js"></script>
  <link rel="stylesheet" crossorigin href="/assets/index-46SMfFz8.css">
</head>
<body>
  <div id="root"></div>
</body>
</html>

```



1 Default Web Page (Follow HTTP Redirection)

port 9090/tcp over SSL

QID: 13910
 Category: CGI
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 11/05/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
 Host: 172.40.123.5:9090
 Connection: Keep-Alive

HTTP/1.1 200 OK
 Server: nginx/1.29.8
 Date: Sat, 25 Apr 2026 01:04:19 GMT
 Content-Type: text/html
 Content-Length: 471
 Last-Modified: Fri, 24 Apr 2026 20:28:05 GMT
 Connection: keep-alive
 ETag: "69ebd255-1d7"
 Accept-Ranges: bytes

```

<!doctype html>
<html lang="en">
<head>

```

```

<meta charset="UTF-8" />
<link rel="icon" type="image/svg+xml" href="/favicon.svg" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />
<title>validacion-documentos</title>
<script type="module" crossorigin src="/assets/index-DdqSzP-5.js"></script>
<link rel="stylesheet" crossorigin href="/assets/index-46SMfFz8.css">
</head>
<body>
  <div id="root"></div>
</body>
</html>

```



1 SSL Server Information Retrieval

port 9090/tcp over SSL

QID: 38116
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 05/24/2016
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM

CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
CAMELLIA128-SHA256	RSA	RSA	SHA256	Camellia(128)	MEDIUM
CAMELLIA256-SHA256	RSA	RSA	SHA256	Camellia(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ARIA128-GCM-SHA256	RSA	RSA	AEAD	ARIAGCM(128)	MEDIUM
ARIA256-GCM-SHA384	RSA	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-ARIA128-GCM-SHA256	ECDH	RSA	AEAD	ARIAGCM(128)	MEDIUM
ECDHE-RSA-ARIA256-GCM-SHA384	ECDH	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-CAMELLIA128-SHA256	ECDH	RSA	SHA256	Camellia(128)	MEDIUM
ECDHE-RSA-CAMELLIA256-SHA384	ECDH	RSA	SHA384	Camellia(256)	HIGH
AES128-CCM	RSA	RSA	AEAD	AESCCM(128)	MEDIUM
AES256-CCM	RSA	RSA	AEAD	AESCCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					



1 SSL Session Caching Information

port 9090/tcp over SSL

QID: 38291
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/19/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 9090/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 9090/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
AES256-SHA256	RSA		2048	no	110	low
AES128-SHA256	RSA		2048	no	110	low
AES256-CCM	RSA		2048	no	110	low
AES128-CCM	RSA		2048	no	110	low
ARIA256-GCM-SHA384	RSA		2048	no	110	low
ARIA128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA256	RSA		2048	no	110	low
AES256-GCM-SHA384	RSA		2048	no	110	low
AES128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA	RSA		2048	no	110	low
CAMELLIA128-SHA	RSA		2048	no	110	low
AES256-SHA	RSA		2048	no	110	low
AES128-SHA	RSA		2048	no	110	low
CAMELLIA128-SHA256	RSA		2048	no	110	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low

ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	x448	448	yes	224	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 9090/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no

1 Secure Sockets Layer (SSL) Certificate Transparency Information

port 9090/tcp over SSL

QID: 38718
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.anla.gov.co, O=U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA, ST=Distrito Capital de Bogot, C=CO			
Certificate	no	(unknown)	(unknown)	d809553b944f7affc816196f9 44f85abb0f8fc5e8755260f15 d12e72bb454b14	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	af67883b57b04edd8fa6d97ef 62ea8eb810ac77160f0245e55 d60c2fe785873a	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	acab30706cebec8431f413d2f 4915f111e422443b1f2a68c4f 3c2b3ba71e02c3	Thu 01 Jan 1970 12:00:00 AM GMT



1 Reports if server supports Post Quantum Cryptographic(PQC) Key Exchange Algorithm

port 9090/tcp over SSL

QID: 38994
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

It reports complete list of all host-supported PQC key-exchange algorithms along with full handshake details.
If server hosts any service

over TLS1.3, then a probe is sent to validate if the service supports following PQC key exchange

algorithms.
MLKEM512
MLKEM768
MLKEM1024
X25519MLKEM768
SecP256r1MLKEM768
SecP384r1MLKEM1024

Field

Description

Cipher name
Cipher used

Protocol
TLS

version

Key-exchange
Negotiated PQC KEX

Authentication

Signature algorithm

MAC
Message authentication code

Encryption + key
strength
Encryption mode and key size

NIST security strength
Security strength (NIST
equivalent)

Reference: <https://csrc.nist.gov/groups/ST/post-quantum-crypto/evaluation-criteria.html>

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	STRENGTH
--------	--------------	----------------	-----	--------------------------	----------

1

Reports Signature Algorithm used in Post Quantum Cryptographic(PQC) detection using QID 38994

port 9090/tcp over SSL

QID:

38995

Category:

General remote services

Associated CVEs:

-

Vendor Reference:

-

Bugtraq ID:

-

Service Modified:

01/05/2026

User Modified:

-

Edited:

No

PCI Vuln:

No

THREAT:

If server hosts any service over TLS1.3, then a probe is sent to validate if the service supports PQC key exchange algorithms as part of QID38994. This QID reports Signature Algorithm used by the service for Post Quantum Cryptographic(PQC) SSL handshake using QID 38994.

It reports server's preferred PQC signature algorithm. This QID is planned for future deprecation.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Preferred PQC Signature Algorithm: RSA-PSS

1

TLS Secure Renegotiation Extension Support Information

port 9090/tcp over SSL

QID:

42350

Category:

General remote services

Associated CVEs:

-

Vendor Reference:

-

Bugtraq ID:

-

Service Modified:

03/21/2016

User Modified:

-

Edited:

No

PCI Vuln:

No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tie renegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 9090/tcp over SSL

QID:	48340
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	SSL/TLS Server supports TLSv1.2
Bugtraq ID:	-
Service Modified:	04/13/2026
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 9090/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	b2:f8:3d:72:1f:f3:a7:29:60:a2:df:c3:eb:8c:4e:fe
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(0)SUBJECT NAME	
countryName	CO
stateOrProvinceName	Distrito Capital de Bogotá\C3\A1
organizationName	U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA
commonName	*.anla.gov.co
(0)Valid From	Oct 22 00:00:00 2025 GMT
(0)Valid Till	Nov 3 23:59:59 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)

(0)	Modulus:
(0)	00:c5:22:80:6e:68:2e:0a:69:6c:67:0c:b8:ee:74:
(0)	e6:56:64:4b:b8:7c:61:47:27:e3:6d:60:a6:34:1e:
(0)	77:20:80:97:2e:ef:ac:2a:8c:52:08:59:9b:33:1e:
(0)	46:70:61:83:8e:1a:85:af:55:76:33:a3:94:c1:04:
(0)	e3:2c:f3:01:07:35:c1:4a:dc:48:47:42:2f:ae:f1:
(0)	fd:b7:49:e5:ff:21:ba:47:cb:bf:1e:4d:13:d3:32:
(0)	17:73:33:65:22:03:ee:2d:36:f2:bc:5a:a5:7d:ad:
(0)	03:01:c2:c0:fe:95:9e:af:81:95:bb:43:59:95:4a:
(0)	bf:82:31:de:e6:1b:43:f4:11:c0:36:be:2c:00:fc:
(0)	2f:97:4b:bb:78:87:61:6e:29:1a:91:8b:a6:2d:f6:
(0)	27:75:93:c2:46:8d:84:cf:b6:8a:69:98:4d:2d:b3:
(0)	4c:1d:44:ea:f6:a4:f9:00:5b:c8:8a:ed:77:66:b3:
(0)	ce:b1:87:b7:e7:52:95:da:e2:08:0d:bb:03:78:02:
(0)	17:46:ce:46:e7:83:f1:1d:ba:47:a3:e2:0e:e3:7b:
(0)	dc:ff:47:79:09:ff:a4:5a:2d:58:4c:d4:1c:24:af:
(0)	a1:aa:ed:50:96:8e:9c:e5:7a:a2:ba:91:53:30:4c:
(0)	42:04:c6:39:7b:c1:f3:88:68:7b:6f:5a:8b:1d:ef:
(0)	5c:5f
(0)	Exponent: 65537 (0x10001)
(0)	X509v3 EXTENSIONS
(0)	X509v3 Authority Key Identifier keyid:E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(0)	X509v3 Subject Key Identifier 3A:B2:87:43:6F:E2:96:F3:ED:40:44:B2:5F:8C:7E:8B:8F:2C:CD:44
(0)	X509v3 Key Usage critical
(0)	Digital Signature, Key Encipherment
(0)	X509v3 Basic Constraints critical
(0)	CA:FALSE
(0)	X509v3 Extended Key Usage TLS Web Server Authentication
(0)	X509v3 Certificate Policies Policy: 1.3.6.1.4.1.6449.1.2.1.3.4
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.2
(0)	X509v3 CRL Distribution Points
(0)	Full Name:
(0)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crl
(0)	Authority Information Access CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
(0)	OCSP - URI:http://ocsp.sectigo.com
(0)	X509v3 Subject Alternative Name DNS:*.anla.gov.co, DNS:anla.gov.co
(0)	CT Precertificate SCTs Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:
(0)	B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14
(0)	Timestamp : Oct 22 21:05:01.112 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:DB:DF:24:6B:4B:B4:A3:AF:88:F0:38:
(0)	D1:3F:21:84:EF:C7:FF:E9:37:FB:FE:CD:B6:CA:04:EF:
(0)	45:22:C8:5B:32:02:21:00:F3:94:94:8C:3F:DA:C9:34:
(0)	51:AE:9A:73:07:1B:37:36:DC:28:62:98:D7:5C:66:52:
(0)	98:71:17:EA:46:23:10:97
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AF:67:88:3B:57:B0:4E:DD:8F:A6:D9:7E:F6:2E:A8:EB:
(0)	81:0A:C7:71:60:F0:24:5E:55:D6:0C:2F:E7:85:87:3A
(0)	Timestamp : Oct 22 21:05:01.223 2025 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:D2:A5:92:31:F6:F8:92:C8:0D:45:20:
(0)	A9:43:B4:3D:09:ED:63:29:FE:6C:BF:13:91:72:85:72:
(0)	ED:AF:05:9C:32:02:20:08:8A:F2:6D:EA:45:68:1A:22:
(0)	08:F4:76:CA:54:F5:B5:75:78:5E:A5:3B:2B:94:42:20:
(0)	03:D1:89:A3:78:FC:78
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AC:AB:30:70:6C:EB:EC:84:31:F4:13:D2:F4:91:5F:11:
(0)	1E:42:24:43:B1:F2:A6:8C:4F:3C:2B:3B:A7:1E:02:C3
(0)	Timestamp : Oct 22 21:05:00.999 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:7A:D5:12:14:07:82:C9:A8:23:A7:95:43:
(0)	83:2B:93:B8:98:74:39:EA:8B:81:EE:6B:D9:1C:CB:DB:
(0)	50:74:D2:BA:02:21:00:C0:5F:F6:05:5B:47:AB:76:2E:
(0)	57:C7:FB:81:9B:91:F0:94:D6:15:89:F5:92:BF:31:F6:
(0)	02:CB:61:FB:61:95:9F
(0)Signature	(384 octets)
(0)	6f:c0:09:87:ec:ea:a5:4c:65:e0:96:7f:ee:cd:75:35
(0)	51:57:14:d5:af:5b:ed:55:e5:c4:27:67:93:7e:af:0a
(0)	ad:d2:a5:b9:86:c9:52:60:fc:8e:01:3c:33:bc:68:e2
(0)	7e:29:00:f6:4b:55:d6:1b:1e:a5:3e:e7:65:02:a5:c5
(0)	9d:6a:a2:d2:7e:68:e5:19:af:6d:81:db:29:c8:c8:6b
(0)	20:fa:eb:0b:70:20:be:bc:bb:89:48:ae:d4:d1:a8:ae
(0)	5c:01:be:87:43:5a:c6:43:b6:4a:de:24:a3:02:3b:67
(0)	d4:03:ab:90:d1:68:e0:7f:c7:f5:7d:15:2c:c7:bd:bd
(0)	35:33:ba:a3:1f:c6:a9:57:aa:a6:c7:ad:98:be:2a:8f
(0)	cb:c2:2e:1e:7f:7c:0f:e4:f0:a0:61:5a:24:66:24:ae
(0)	19:1c:8b:9f:3a:bc:a1:b4:47:71:63:43:2c:01:59:7c
(0)	9a:6a:88:aa:5f:f4:91:4a:7f:28:08:7b:61:52:4b:da
(0)	20:a9:e7:0e:35:a9:87:c5:1c:74:86:d2:56:7a:87:eb
(0)	03:73:4c:44:6e:c8:fd:b0:d0:f6:1f:d0:69:82:ab:57
(0)	d4:6d:2c:d7:7b:5a:60:ce:20:2a:6a:1f:0f:43:2a:79
(0)	f0:74:86:d8:6c:dc:86:a5:ca:98:d8:ae:38:79:36:38
(0)	2d:a1:02:36:5d:c2:04:3f:1a:f5:ea:00:99:b7:78:0c
(0)	fe:36:07:9b:5d:21:f9:14:65:37:d8:d8:e5:fd:ee:1a
(0)	c0:c3:a8:d7:0d:d5:a8:d2:0b:da:c5:c8:39:03:52:1d
(0)	84:ec:2d:67:f9:c1:7d:79:56:0b:8d:b4:b8:74:30:63
(0)	4c:02:98:d1:6a:0b:76:e9:72:2d:90:78:ac:96:88:a0
(0)	64:04:46:cd:3f:75:64:2a:79:14:a5:88:48:6d:ed:a2
(0)	e5:8b:eb:10:91:9c:05:2a:32:20:d3:d5:a7:d8:16:1d
(0)	4f:c1:91:ed:6d:93:a3:00:8d:b8:26:d0:cc:47:cf:57
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(1)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36

(1)Valid From	Mar 22 00:00:00 2021 GMT
(1)Valid Till	Mar 21 23:59:59 2036 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(3072 bit)
(1)	RSA Public-Key: (3072 bit)
(1)	Modulus:
(1)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(1)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(1)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(1)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(1)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(1)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(1)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(1)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(1)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(1)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(1)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(1)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(1)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(1)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(1)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(1)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(1)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(1)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(1)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(1)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(1)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(1)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(1)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(1)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(1)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(1)	36:d7:77:f5:91:27:08:66:7b:4d
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(1)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	Policy: 2.23.140.1.2.2
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(1)	OCSP - URI:http://ocsp.sectigo.com
(1)Signature	(512 octets)
(1)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(1)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(1)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(1)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(1)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(1)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11

(1)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(1)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(1)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(1)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(1)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(1)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(1)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(1)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(1)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(1)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(1)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(1)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(1)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(1)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(1)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(1)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(1)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(1)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(1)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(1)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(1)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(1)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(1)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(1)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(1)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(1)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(2)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(2)Valid From	Mar 22 00:00:00 2021 GMT
(2)Valid Till	Jan 18 23:59:59 2038 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(2)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(2)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(2)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(2)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(2)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(2)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(2)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(2)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:

(2)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(2)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(2)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(2)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(2)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(2)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(2)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(2)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(2)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(2)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(2)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(2)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(2)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(2)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(2)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(2)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(2)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(2)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(2)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(2)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(2)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(2)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(2)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(2)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(2)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(2)	7c:6d:cf
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(2)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(2)Signature	(512 octets)
(2)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(2)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(2)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(2)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(2)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(2)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(2)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(2)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(2)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(2)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(2)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(2)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(2)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(2)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17

(2)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(2)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(2)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(2)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(2)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(2)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(2)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(2)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(2)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(2)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(2)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(2)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(2)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(2)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(2)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(2)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(2)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(2)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(3)CERTIFICATE 3	
(3)Version	3 (0x2)
(3)Serial Number	01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d
(3)Signature Algorithm	sha384WithRSAEncryption
(3)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)SUBJECT NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)Valid From	Feb 1 00:00:00 2010 GMT
(3)Valid Till	Jan 18 23:59:59 2038 GMT
(3)Public Key Algorithm	rsaEncryption
(3)RSA Public Key	(4096 bit)
(3)	RSA Public-Key: (4096 bit)
(3)	Modulus:
(3)	00:80:12:65:17:36:0e:c3:db:08:b3:d0:ac:57:0d:
(3)	76:ed:cd:27:d3:4c:ad:50:83:61:e2:aa:20:4d:09:
(3)	2d:64:09:dc:ce:89:9f:cc:3d:a9:ec:f6:cf:c1:dc:
(3)	f1:d3:b1:d6:7b:37:28:11:2b:47:da:39:c6:bc:3a:
(3)	19:b4:5f:a6:bd:7d:9d:a3:63:42:b6:76:f2:a9:3b:
(3)	2b:91:f8:e2:6f:d0:ec:16:20:90:09:3e:e2:e8:74:
(3)	c9:18:b4:91:d4:62:64:db:7f:a3:06:f1:88:18:6a:
(3)	90:22:3c:bc:fe:13:f0:87:14:7b:f6:e4:1f:8e:d4:
(3)	e4:51:c6:11:67:46:08:51:cb:86:14:54:3f:bc:33:
(3)	fe:7e:6c:9c:ff:16:9d:18:bd:51:8e:35:a6:a7:66:
(3)	c8:72:67:db:21:66:b1:d4:9b:78:03:c0:50:3a:e8:
(3)	cc:f0:dc:bc:9e:4c:fe:af:05:96:35:1f:57:5a:b7:
(3)	ff:ce:f9:3d:b7:2c:b6:f6:54:dd:c8:e7:12:3a:4d:
(3)	ae:4c:8a:b7:5c:9a:b4:b7:20:3d:ca:7f:22:34:ae:
(3)	7e:3b:68:66:01:44:e7:01:4e:46:53:9b:33:60:f7:

(3)	94:be:53:37:90:73:43:f3:32:c3:53:ef:db:aa:fe:
(3)	74:4e:69:c7:6b:8c:60:93:de:c4:c7:0c:df:e1:32:
(3)	ae:cc:93:3b:51:78:95:67:8b:ee:3d:56:fe:0c:d0:
(3)	69:0f:1b:0f:f3:25:26:6b:33:6d:f7:6e:47:fa:73:
(3)	43:e5:7e:0e:a5:66:b1:29:7c:32:84:63:55:89:c4:
(3)	0d:c1:93:54:30:19:13:ac:d3:7d:37:a7:eb:5d:3a:
(3)	6c:35:5c:db:41:d7:12:da:a9:49:0b:df:d8:80:8a:
(3)	09:93:62:8e:b5:66:cf:25:88:cd:84:b8:b1:3f:a4:
(3)	39:0f:d9:02:9e:eb:12:4c:95:7c:f3:6b:05:a9:5e:
(3)	16:83:cc:b8:67:e2:e8:13:9d:cc:5b:82:d3:4c:b3:
(3)	ed:5b:ff:de:e5:73:ac:23:3b:2d:00:bf:35:55:74:
(3)	09:49:d8:49:58:1a:7f:92:36:e6:51:92:0e:f3:26:
(3)	7d:1c:4d:17:bc:c9:ec:43:26:d0:bf:41:5f:40:a9:
(3)	44:44:f4:99:e7:57:87:9e:50:1f:57:54:a8:3e:fd:
(3)	74:63:2f:b1:50:65:09:e6:58:42:2e:43:1a:4c:b4:
(3)	f0:25:47:59:fa:04:1e:93:d4:26:46:4a:50:81:b2:
(3)	de:be:78:b7:fc:67:15:e1:c9:57:84:1e:0f:63:d6:
(3)	e9:62:ba:d6:5f:55:2e:ea:5c:c6:28:08:04:25:39:
(3)	b8:0e:2b:a9:f2:4c:97:1c:07:3f:0d:52:f5:ed:ef:
(3)	2f:82:0f
(3)	Exponent: 65537 (0x10001)
(3)X509v3 EXTENSIONS	
(3)X509v3 Subject Key Identifier	53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(3)X509v3 Key Usage	critical
(3)	Certificate Sign, CRL Sign
(3)X509v3 Basic Constraints	critical
(3)	CA:TRUE
(3)Signature	(512 octets)
(3)	5c:d4:7c:0d:cf:f7:01:7d:41:99:65:0c:73:c5:52:9f
(3)	cb:f8:cf:99:06:7f:1b:da:43:15:9f:9e:02:55:57:96
(3)	14:f1:52:3c:27:87:94:28:ed:1f:3a:01:37:a2:76:fc
(3)	53:50:c0:84:9b:c6:6b:4e:ba:8c:21:4f:a2:8e:55:62
(3)	91:f3:69:15:d8:bc:88:e3:c4:aa:0b:fd:ef:a8:e9:4b
(3)	55:2a:06:20:6d:55:78:29:19:ee:5f:30:5c:4b:24:11
(3)	55:ff:24:9a:6e:5e:2a:2b:ee:0b:4d:9f:7f:f7:01:38
(3)	94:14:95:43:07:09:fb:60:a9:ee:1c:ab:12:8c:a0:9a
(3)	5e:a7:98:6a:59:6d:8b:3f:08:fb:c8:d1:45:af:18:15
(3)	64:90:12:0f:73:28:2e:c5:e2:24:4e:fc:58:ec:f0:f4
(3)	45:fe:22:b3:eb:2f:8e:d2:d9:45:61:05:c1:97:6f:a8
(3)	76:72:8f:8b:8c:36:af:bf:0d:05:ce:71:8d:e6:a6:6f
(3)	1f:6c:a6:71:62:c5:d8:d0:83:72:0c:f1:67:11:89:0c
(3)	9c:13:4c:72:34:df:bc:d5:71:df:aa:71:dd:e1:b9:6c
(3)	8c:3c:12:5d:65:da:bd:57:12:b6:43:6b:ff:e5:de:4d
(3)	66:11:51:cf:99:ae:ec:17:b6:e8:71:91:8c:de:49:fe
(3)	dd:35:71:a2:15:27:94:1c:cf:61:e3:26:bb:6f:a3:67
(3)	25:21:5d:e6:dd:1d:0b:2e:68:1b:3b:82:af:ec:83:67
(3)	85:d4:98:51:74:b1:b9:99:80:89:ff:7f:78:19:5c:79
(3)	4a:60:2e:92:40:ae:4c:37:2a:2c:c9:c7:62:c8:0e:5d
(3)	f7:36:5b:ca:e0:25:25:01:b4:dd:1a:07:9c:77:00:3f
(3)	d0:dc:d5:ec:3d:d4:fa:bb:3f:cc:85:d6:6f:7f:a9:2d
(3)	df:b9:02:f7:f5:97:9a:b5:35:da:c3:67:b0:87:4a:a9
(3)	28:9e:23:8e:ff:5c:27:6b:e1:b0:4f:f3:07:ee:00:2e
(3)	d4:59:87:cb:52:41:95:ea:f4:47:d7:ee:64:41:55:7c
(3)	8d:59:02:95:dd:62:9d:c2:b9:ee:5a:28:74:84:a5:9b
(3)	b7:90:c7:0c:07:df:f5:89:36:74:32:d6:28:c1:b0:b0

(3)	0b:e0:9c:4c:c3:1c:d6:fc:e3:69:b5:47:46:81:2f:a2
(3)	82:ab:d3:63:44:70:c4:8d:ff:2d:33:ba:ad:8f:7b:b5
(3)	70:88:ae:3e:19:cf:40:28:d8:fc:c8:90:bb:5d:99:22
(3)	f5:52:e6:58:c5:1f:88:31:43:ee:88:1d:d7:c6:8e:3c
(3)	43:6a:1d:a7:18:de:7d:3d:16:f1:62:f9:ca:90:a8:fd
(4)CERTIFICATE 4	
(4)Version	3 (0x2)
(4)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(4)Signature Algorithm	sha384WithRSAEncryption
(4)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(4)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(4)Valid From	Mar 22 00:00:00 2021 GMT
(4)Valid Till	Jan 18 23:59:59 2038 GMT
(4)Public Key Algorithm	rsaEncryption
(4)RSA Public Key	(4096 bit)
(4)	RSA Public-Key: (4096 bit)
(4)	Modulus:
(4)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(4)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(4)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(4)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(4)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(4)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(4)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(4)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(4)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(4)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(4)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(4)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(4)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(4)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(4)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(4)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(4)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(4)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(4)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(4)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(4)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(4)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(4)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(4)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(4)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(4)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(4)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(4)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(4)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(4)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:

(4)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(4)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(4)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(4)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(4)	7c:6d:cf
(4)	Exponent: 65537 (0x10001)
(4)X509v3 EXTENSIONS	
(4)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(4)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(4)X509v3 Key Usage	critical
(4)	Digital Signature, Certificate Sign, CRL Sign
(4)X509v3 Basic Constraints	critical
(4)	CA:TRUE
(4)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(4)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(4)X509v3 CRL Distribution Points	
(4)	Full Name:
(4)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(4)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(4)Signature	(512 octets)
(4)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(4)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(4)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(4)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(4)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(4)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(4)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(4)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(4)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(4)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(4)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(4)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(4)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(4)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(4)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(4)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(4)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(4)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(4)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(4)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(4)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(4)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(4)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(4)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(4)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(4)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(4)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(4)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(4)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(4)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(4)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(4)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(5)CERTIFICATE 5	
(5)Version	3 (0x2)
(5)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71

(5)Signature Algorithm	sha384WithRSAEncryption
(5)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(5)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(5)Valid From	Mar 22 00:00:00 2021 GMT
(5)Valid Till	Mar 21 23:59:59 2036 GMT
(5)Public Key Algorithm	rsaEncryption
(5)RSA Public Key	(3072 bit)
(5)	RSA Public-Key: (3072 bit)
(5)	Modulus:
(5)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(5)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(5)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(5)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(5)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(5)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(5)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(5)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(5)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(5)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(5)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(5)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(5)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(5)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(5)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(5)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(5)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(5)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(5)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(5)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(5)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(5)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(5)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(5)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(5)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(5)	36:d7:77:f5:91:27:08:66:7b:4d
(5)	Exponent: 65537 (0x10001)
(5)X509v3 EXTENSIONS	
(5)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(5)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(5)X509v3 Key Usage	critical
(5)	Digital Signature, Certificate Sign, CRL Sign
(5)X509v3 Basic Constraints	critical
(5)	CA:TRUE, pathlen:0
(5)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(5)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(5)	Policy: 2.23.140.1.2.2
(5)X509v3 CRL Distribution Points	
(5)	Full Name:
(5)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl

(5)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(5)	OCSP - URI:http://ocsp.sectigo.com
(5)Signature	(512 octets)
(5)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(5)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(5)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(5)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(5)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(5)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(5)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(5)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(5)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(5)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(5)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(5)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(5)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(5)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(5)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(5)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(5)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(5)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(5)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(5)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(5)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(5)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(5)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(5)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(5)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(5)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(5)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(5)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(5)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(5)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(5)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(5)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c

1 Web Server Supports HTTP Request Pipelining

port 9090/tcp over SSL

QID: 86565
 Category: Web server
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 02/22/2005
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:9090

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:9090

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:40:54 GMT
Content-Type: text/html
Content-Length: 471
Last-Modified: Fri, 24 Apr 2026 20:28:05 GMT
Connection: keep-alive
ETag: "69ebd255-1d7"
Accept-Ranges: bytes

```
<!doctype html>
<html lang="en">
<head>
  <meta charset="UTF-8" />
  <link rel="icon" type="image/svg+xml" href="/favicon.svg" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>validacion-documentos</title>
  <script type="module" crossorigin src="/assets/index-DdqSzP-5.js"></script>
  <link rel="stylesheet" crossorigin href="/assets/index-46SMfFz8.css">
</head>
<body>
  <div id="root"></div>
</body>
</html>
```

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:40:54 GMT
Content-Type: text/html
Content-Length: 471
Last-Modified: Fri, 24 Apr 2026 20:28:05 GMT
Connection: keep-alive
ETag: "69ebd255-1d7"
Accept-Ranges: bytes

```
<!doctype html>
<html lang="en">
<head>
  <meta charset="UTF-8" />
  <link rel="icon" type="image/svg+xml" href="/favicon.svg" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>validacion-documentos</title>
  <script type="module" crossorigin src="/assets/index-DdqSzP-5.js"></script>
  <link rel="stylesheet" crossorigin href="/assets/index-46SMfFz8.css">
</head>
<body>
```

```
<div id="root"></div>
</body>
</html>
```

1 Default Web Page

port 25000/tcp over SSL

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:25000
Connection: Keep-Alive

```
{"error": "Not found"}
```

1 Default Web Page (Follow HTTP Redirection)

port 25000/tcp over SSL

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:25000
Connection: Keep-Alive

{"error": "Not found"}



1 SSL Server Information Retrieval

port 25000/tcp over SSL

QID: 38116
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH



1 SSL Session Caching Information

port 25000/tcp over SSL

QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is disabled on the target.

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 25000/tcp over SSL

QID:

38597

Category:

General remote services

Associated CVEs:

-

Vendor Reference:

-

Bugtraq ID:

-

Service Modified:

07/12/2021

User Modified:

-

Edited:

No

PCI Vuln:

No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	rejected
0399	rejected
0400	rejected
0499	rejected

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 25000/tcp over SSL

QID:

38704

Category:

General remote services

Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
AES256-GCM-SHA384	RSA		2048	no	110	low
AES128-GCM-SHA256	RSA		2048	no	110	low
AES256-SHA	RSA		2048	no	110	low
AES128-SHA	RSA		2048	no	110	low
DES-CBC3-SHA	RSA		2048	no	110	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low

ECDHE-RSA-DES-CBC3-SHA	ECDHE x25519	256	yes	128	low
ECDHE-RSA-DES-CBC3-SHA	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-DES-CBC3-SHA	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-DES-CBC3-SHA	ECDHE secp521r1	521	yes	260	low
TLSv1.3					



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 25000/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client and server
OCSP stapling	no
SCT extension	no

TLSv1.3	
Heartbeat	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

1 TLS Secure Renegotiation Extension Support Information

port 25000/tcp over SSL

QID: 42350
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/21/2016
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tie renegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 25000/tcp over SSL

QID: 48340
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
 Bugtraq ID: -
 Service Modified: 04/13/2026
 User Modified: -

Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported

 1 SSL Certificate - Information

port 25000/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	32:0a:a3:a1:92:00:ef:fb:65:a1:31:61:fb:16:87:ce:8d:19:8a:62
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
commonName	10.152.183.1
(0)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Canonical
localityName	Canonical
organizationName	Canonical
organizationalUnitName	Canonical
commonName	127.0.0.1
(0)Valid From	Apr 24 20:28:10 2026 GMT
(0)Valid Till	Apr 24 20:28:10 2027 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:b7:4d:45:8d:ee:6e:50:03:da:8b:b3:6a:0f:77:
(0)	18:c5:04:9a:43:65:93:ce:31:89:8b:6f:59:2f:74:
(0)	43:82:5a:91:3d:c0:83:6a:2b:3c:f9:d9:ab:da:26:
(0)	ba:8c:70:8d:7f:52:cb:be:44:5b:74:3c:78:11:b8:
(0)	6d:c2:27:74:2f:8c:e5:52:33:b2:f7:80:54:18:43:
(0)	ca:71:ec:4d:3a:f6:00:60:33:fd:88:09:e2:8c:8f:
(0)	1f:5a:f9:bf:04:01:3f:a4:2c:92:c7:6e:75:45:94:
(0)	12:44:c4:70:13:86:23:a3:89:81:67:2b:02:e2:af:
(0)	60:5f:4a:6b:d2:db:4f:e4:30:6b:8a:f3:24:54:6b:
(0)	ab:80:32:0e:c5:e9:c5:ae:50:c1:6c:47:96:f3:09:
(0)	b0:95:6d:e6:1b:d1:a9:b4:74:c0:32:84:3d:f6:eb:
(0)	c8:42:1f:74:f1:b8:8f:49:e1:67:82:57:80:1c:33:
(0)	5c:21:f1:f8:d8:de:d5:ee:ec:3e:61:6f:73:4f:b5:
(0)	9d:49:92:fe:b4:aa:d8:20:32:03:b9:c4:68:0b:de:
(0)	e0:a7:8f:fd:62:5d:a8:8f:1d:4c:50:b2:5f:62:18:
(0)	5c:de:cb:5c:0c:98:66:32:a3:e8:48:d6:38:00:14:
(0)	9f:64:e0:e3:1b:34:6e:05:0d:1c:52:af:2a:01:96:
(0)	59:93
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:DF:26:75:FC:23:27:11:01:4D:6E:D9:A3:E5:E9:92:99:7E:A6:9B:02
(0)	DirName:/CN=10.152.183.1
(0)	serial:17:14:7C:06:1F:0B:81:4C:70:C4:86:13:33:1A:52:88:FC:CD:D1:71
(0)X509v3 Basic Constraints	CA:FALSE
(0)X509v3 Key Usage	Digital Signature, Key Encipherment, Data Encipherment
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Subject Alternative Name	DNS:kubernetes, DNS:kubernetes.default, DNS:kubernetes.default.svc, DNS:kubernetes.default.svc.cluster, DNS:kubernetes.default.svc.cluster.local, IP Address:127.0.0.1, IP Address:10.152.183.1, IP Address:172.40.123.5, IP Address:172.18.0.1, IP Address:172.19.0.1, IP Address:172.20.0.1, IP Address:172.21.0.1, IP Address:172.23.0.1, IP Address:172.26.0.1, IP Address:172.25.0.1, IP Address:172.22.0.1, IP Address:172.24.0.1
(0)Signature	(256 octets)
(0)	74:38:32:da:6e:89:79:dc:9a:2a:d8:8b:d3:a6:1f:98

(0)	e1:35:26:c0:8c:dc:d2:6b:84:84:38:12:d6:a5:ab:66
(0)	7e:ef:25:0d:b2:6b:3f:8c:9f:da:69:41:49:e2:50:2f
(0)	d3:7a:ed:29:ca:8a:6a:46:1c:80:7e:74:88:4f:66:c1
(0)	ca:dc:af:a3:4b:0d:27:a7:bc:15:b9:eb:f2:4e:58:3f
(0)	30:34:43:27:9c:5a:14:4b:13:cc:8c:cb:a9:19:82:89
(0)	a6:2d:6d:55:52:4c:b8:e1:4b:64:e4:8d:09:4f:94:ad
(0)	2a:9f:63:de:4c:3c:30:c1:f0:a4:24:62:ee:fa:00:d6
(0)	6d:8e:e3:64:5c:59:f4:17:4e:2c:68:71:36:fd:d7:39
(0)	d5:96:7c:f1:5c:91:f4:b7:f0:ab:79:53:0f:71:4a:df
(0)	eb:87:4e:81:a8:f0:c5:14:e8:d3:b0:bc:80:98:bd:fa
(0)	b6:e2:05:1f:c0:07:da:d0:b0:1c:39:8d:db:26:00:f2
(0)	cd:8f:f5:a9:0d:90:50:2a:a3:b6:17:57:ad:83:83:06
(0)	f0:8c:f6:3c:f1:92:be:51:f8:4f:6f:85:9f:bb:81:ff
(0)	4e:51:7b:bc:b0:24:3f:1a:c7:ef:6a:98:06:e0:45:d3
(0)	34:64:20:30:a7:ad:1f:6d:69:d3:51:62:78:e9:3a:7a



1 HTTP Response Method and Header Information Collected

port 25000/tcp

QID: 48118
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 25000.

GET / HTTP/1.1
Host: 172.40.123.5:25000

Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Sat, 25 Apr 2026 01:20:36 GMT
Content-Length: 21
Content-Type: text/plain; charset=utf-8

1 Default Web Page

port 8089/tcp over SSL

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8089
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 01:29:04 GMT
Content-Type: text/html
Content-Length: 2706
Last-Modified: Fri, 10 Apr 2026 18:57:21 GMT
Connection: keep-alive
ETag: "69d94811-a92"
Accept-Ranges: bytes

```
<!doctype html>
<html lang="es">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <title>Reporte PAI Frontend</title>
  <link rel="stylesheet" href="styles.css" />
```

```

</head>
<body>
  <header>
    <div class="brand">
      <svg viewBox="0 0 24 24" width="22" height="22" aria-hidden="true"><path fill="currentColor" d="M19 3H5a2 2 0 0 0-2 2v14a2 2 0 0 0 2 2h14a2 2 0 0 0 2 2v5a2 2 0 0 0 2 2Zm-7 14H7v-2h5v2Zm5-4H7v-2h10v2Zm0-4H7V7h10v2Z"/></svg>
      <span>Reporte PAI</span>
    </div>
  </header>

  <main>
    <h1 class="page-title">
      <svg viewBox="0 0 24 24" width="22" height="22" aria-hidden="true"><path fill="currentColor" d="M12 2a10 10 0 1 0 10 10A10.011 10.011 0 0 0 12 2Zm1 14h-2v-2h2Zm0-4h-2V6h2Z"/></svg>
      Validacin de Documentos
    </h1>
    <p class="subtitle">Sube tu archivo y procesaremos automticamente el informe.</p>

    <section class="card">
      <h2>Archivo a procesar</h2>

      <div class="row">
        <label for="corte_mes">Corte de mes</label>
        <div class="input-inline">
          <input id="corte_mes" name="corte_mes" type="text"
            placeholder="YYYY-MM o YYYY-MM-DD o marzo 2026" />
          <button id="btn-fill" type="button" title="Usar mes actual"></button>
        </div>
        <small class="hint">Tip: usa <b>YYYY-MM</b> para corte mensual.</small>
      </div>

      <div id="dropzone" class="dropzone" tabindex="0" role="button" aria-label="Zona para arrastrar y soltar archivo">
        <div class="dz-inner">
          <svg viewBox="0 0 24 24" width="38" height="38" aria-hidden="true"><path fill="currentColor" d="M19 12v7H5v-7H3v7a2 2 0 0 0 2 2h14a2 2 0 0 0 2 2v-7ZM11 6.414 8.707 7.293 7.293 12 2.586 4.707 4.707 1.414 1.414 13 6.414V16h-2Z"/></svg>
          <p class="dz-title">Arrastra tu archivo aqu</p>
          <p class="dz-help">o haz clic para seleccionar</p>
          <p class="dz-note">Formato: XLSX (mx. 20MB)</p>
        </div>
        <input id="file" type="file" accept=".xlsx" aria-label="Seleccionar archivo" />
      </div>

      <div class="file-chip" id="file-chip" hidden>
        <span id="file-name"></span>
        <button id="btn-clear" type="button" aria-label="Quitar archivo"></button>
      </div>

      <div class="actions">
        <button id="btn-process" type="button" disabled>Procesar documento</button>
      </div>

      <div id="status" class="status" role="status" aria-live="polite"></div>
      <div id="result" class="result"></div>
    </section>
  </main>

  <footer>
    <small> Reporte PAI Frontend</small>
  </footer>

  <script src="app.js"></script>
</body>
</html>

```



1 Default Web Page (Follow HTTP Redirection)

port 8089/tcp over SSL

QID: 13910
 Category: CGI
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 11/05/2020
 User Modified: -
 Edited: No

PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8089
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 01:31:10 GMT
Content-Type: text/html
Content-Length: 2706
Last-Modified: Fri, 10 Apr 2026 18:57:21 GMT
Connection: keep-alive
ETag: "69d94811-a92"
Accept-Ranges: bytes

```
<!doctype html>
<html lang="es">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <title>Reporte PAI Frontend</title>
  <link rel="stylesheet" href="styles.css" />
</head>
<body>
  <header>
    <div class="brand">
      <svg viewBox="0 0 24 24" width="22" height="22" aria-hidden="true"><path fill="currentColor" d="M19 3H5a2 2 0 0 2 2v14a2 2 0 0 2 2V5a2 2 0 0 2 2Zm-7 14H7v-2h5v2Zm5-4H7v-2h10v2Zm0-4H7V7h10v2Z"/></svg>
      <span>Reporte PAI</span>
    </div>
  </header>

  <main>
    <h1 class="page-title">
      <svg viewBox="0 0 24 24" width="22" height="22" aria-hidden="true"><path fill="currentColor" d="M12 2a10 10 0 1 0 10 10.011 10.011 0 0 1 2Zm1 14h-2v-2h2Zm0-4h-2V6h2Z"/></svg>
      Validacin de Documentos
    </h1>
    <p class="subtitle">Sube tu archivo y procesaremos automticamente el informe.</p>

    <section class="card">
      <h2>Archivo a procesar</h2>
```

```

<div class="row">
  <label for="corte_mes">Corte de mes</label>
  <div class="input-inline">
    <input id="corte_mes" name="corte_mes" type="text"
      placeholder="YYYY-MM o YYYY-MM-DD o marzo 2026" />
    <button id="btn-fill" type="button" title="Usar mes actual"></button>
  </div>
  <small class="hint">Tip: usa <b>YYYY-MM</b> para corte mensual.</small>
</div>

<div id="dropzone" class="dropzone" tabindex="0" role="button" aria-label="Zona para arrastrar y soltar archivo">
  <div class="dz-inner">
    <svg viewBox="0 0 24 24" width="38" height="38" aria-hidden="true"><path fill="currentColor" d="M19 12v7H5v-7H3v7H5v-7H7v7H9v-7H11v7H13v-7H15v7H17v-7H19v7H21v-7H23v7H25v-7H27v7H29v-7H31v7H33v-7H35v7H37v-7H39v7H41v-7H43v7H45v-7H47v7H49v-7H51v7H53v-7H55v7H57v-7H59v7H61v-7H63v7H65v-7H67v7H69v-7H71v7H73v-7H75v7H77v-7H79v7H81v-7H83v7H85v-7H87v7H89v-7H91v7H93v-7H95v7H97v-7H99v7H101v-7H103v7H105v-7H107v7H109v-7H111v7H113v-7H115v7H117v-7H119v7H121v-7H123v7H125v-7H127v7H129v-7H131v7H133v-7H135v7H137v-7H139v7H141v-7H143v7H145v-7H147v7H149v-7H151v7H153v-7H155v7H157v-7H159v7H161v-7H163v7H165v-7H167v7H169v-7H171v7H173v-7H175v7H177v-7H179v7H181v-7H183v7H185v-7H187v7H189v-7H191v7H193v-7H195v7H197v-7H199v7H201v-7H203v7H205v-7H207v7H209v-7H211v7H213v-7H215v7H217v-7H219v7H221v-7H223v7H225v-7H227v7H229v-7H231v7H233v-7H235v7H237v-7H239v7H241v-7H243v7H245v-7H247v7H249v-7H251v7H253v-7H255v7H257v-7H259v7H261v-7H263v7H265v-7H267v7H269v-7H271v7H273v-7H275v7H277v-7H279v7H281v-7H283v7H285v-7H287v7H289v-7H291v7H293v-7H295v7H297v-7H299v7H301v-7H303v7H305v-7H307v7H309v-7H311v7H313v-7H315v7H317v-7H319v7H321v-7H323v7H325v-7H327v7H329v-7H331v7H333v-7H335v7H337v-7H339v7H341v-7H343v7H345v-7H347v7H349v-7H351v7H353v-7H355v7H357v-7H359v7H361v-7H363v7H365v-7H367v7H369v-7H371v7H373v-7H375v7H377v-7H379v7H381v-7H383v7H385v-7H387v7H389v-7H391v7H393v-7H395v7H397v-7H399v7H401v-7H403v7H405v-7H407v7H409v-7H411v7H413v-7H415v7H417v-7H419v7H421v-7H423v7H425v-7H427v7H429v-7H431v7H433v-7H435v7H437v-7H439v7H441v-7H443v7H445v-7H447v7H449v-7H451v7H453v-7H455v7H457v-7H459v7H461v-7H463v7H465v-7H467v7H469v-7H471v7H473v-7H475v7H477v-7H479v7H481v-7H483v7H485v-7H487v7H489v-7H491v7H493v-7H495v7H497v-7H499v7H501v-7H503v7H505v-7H507v7H509v-7H511v7H513v-7H515v7H517v-7H519v7H521v-7H523v7H525v-7H527v7H529v-7H531v7H533v-7H535v7H537v-7H539v7H541v-7H543v7H545v-7H547v7H549v-7H551v7H553v-7H555v7H557v-7H559v7H561v-7H563v7H565v-7H567v7H569v-7H571v7H573v-7H575v7H577v-7H579v7H581v-7H583v7H585v-7H587v7H589v-7H591v7H593v-7H595v7H597v-7H599v7H601v-7H603v7H605v-7H607v7H609v-7H611v7H613v-7H615v7H617v-7H619v7H621v-7H623v7H625v-7H627v7H629v-7H631v7H633v-7H635v7H637v-7H639v7H641v-7H643v7H645v-7H647v7H649v-7H651v7H653v-7H655v7H657v-7H659v7H661v-7H663v7H665v-7H667v7H669v-7H671v7H673v-7H675v7H677v-7H679v7H681v-7H683v7H685v-7H687v7H689v-7H691v7H693v-7H695v7H697v-7H699v7H701v-7H703v7H705v-7H707v7H709v-7H711v7H713v-7H715v7H717v-7H719v7H721v-7H723v7H725v-7H727v7H729v-7H731v7H733v-7H735v7H737v-7H739v7H741v-7H743v7H745v-7H747v7H749v-7H751v7H753v-7H755v7H757v-7H759v7H761v-7H763v7H765v-7H767v7H769v-7H771v7H773v-7H775v7H777v-7H779v7H781v-7H783v7H785v-7H787v7H789v-7H791v7H793v-7H795v7H797v-7H799v7H801v-7H803v7H805v-7H807v7H809v-7H811v7H813v-7H815v7H817v-7H819v7H821v-7H823v7H825v-7H827v7H829v-7H831v7H833v-7H835v7H837v-7H839v7H841v-7H843v7H845v-7H847v7H849v-7H851v7H853v-7H855v7H857v-7H859v7H861v-7H863v7H865v-7H867v7H869v-7H871v7H873v-7H875v7H877v-7H879v7H881v-7H883v7H885v-7H887v7H889v-7H891v7H893v-7H895v7H897v-7H899v7H901v-7H903v7H905v-7H907v7H909v-7H911v7H913v-7H915v7H917v-7H919v7H921v-7H923v7H925v-7H927v7H929v-7H931v7H933v-7H935v7H937v-7H939v7H941v-7H943v7H945v-7H947v7H949v-7H951v7H953v-7H955v7H957v-7H959v7H961v-7H963v7H965v-7H967v7H969v-7H971v7H973v-7H975v7H977v-7H979v7H981v-7H983v7H985v-7H987v7H989v-7H991v7H993v-7H995v7H997v-7H999v7H1001v-7H1003v7H1005v-7H1007v7H1009v-7H1011v7H1013v-7H1015v7H1017v-7H1019v7H1021v-7H1023v7H1025v-7H1027v7H1029v-7H1031v7H1033v-7H1035v7H1037v-7H1039v7H1041v-7H1043v7H1045v-7H1047v7H1049v-7H1051v7H1053v-7H1055v7H1057v-7H1059v7H1061v-7H1063v7H1065v-7H1067v7H1069v-7H1071v7H1073v-7H1075v7H1077v-7H1079v7H1081v-7H1083v7H1085v-7H1087v7H1089v-7H1091v7H1093v-7H1095v7H1097v-7H1099v7H1101v-7H1103v7H1105v-7H1107v7H1109v-7H1111v7H1113v-7H1115v7H1117v-7H1119v7H1121v-7H1123v7H1125v-7H1127v7H1129v-7H1131v7H1133v-7H1135v7H1137v-7H1139v7H1141v-7H1143v7H1145v-7H1147v7H1149v-7H1151v7H1153v-7H1155v7H1157v-7H1159v7H1161v-7H1163v7H1165v-7H1167v7H1169v-7H1171v7H1173v-7H1175v7H1177v-7H1179v7H1181v-7H1183v7H1185v-7H1187v7H1189v-7H1191v7H1193v-7H1195v7H1197v-7H1199v7H1201v-7H1203v7H1205v-7H1207v7H1209v-7H1211v7H1213v-7H1215v7H1217v-7H1219v7H1221v-7H1223v7H1225v-7H1227v7H1229v-7H1231v7H1233v-7H1235v7H1237v-7H1239v7H1241v-7H1243v7H1245v-7H1247v7H1249v-7H1251v7H1253v-7H1255v7H1257v-7H1259v7H1261v-7H1263v7H1265v-7H1267v7H1269v-7H1271v7H1273v-7H1275v7H1277v-7H1279v7H1281v-7H1283v7H1285v-7H1287v7H1289v-7H1291v7H1293v-7H1295v7H1297v-7H1299v7H1301v-7H1303v7H1305v-7H1307v7H1309v-7H1311v7H1313v-7H1315v7H1317v-7H1319v7H1321v-7H1323v7H1325v-7H1327v7H1329v-7H1331v7H1333v-7H1335v7H1337v-7H1339v7H1341v-7H1343v7H1345v-7H1347v7H1349v-7H1351v7H1353v-7H1355v7H1357v-7H1359v7H1361v-7H1363v7H1365v-7H1367v7H1369v-7H1371v7H1373v-7H1375v7H1377v-7H1379v7H1381v-7H1383v7H1385v-7H1387v7H1389v-7H1391v7H1393v-7H1395v7H1397v-7H1399v7H1401v-7H1403v7H1405v-7H1407v7H1409v-7H1411v7H1413v-7H1415v7H1417v-7H1419v7H1421v-7H1423v7H1425v-7H1427v7H1429v-7H1431v7H1433v-7H1435v7H1437v-7H1439v7H1441v-7H1443v7H1445v-7H1447v7H1449v-7H1451v7H1453v-7H1455v7H1457v-7H1459v7H1461v-7H1463v7H1465v-7H1467v7H1469v-7H1471v7H1473v-7H1475v7H1477v-7H1479v7H1481v-7H1483v7H1485v-7H1487v7H1489v-7H1491v7H1493v-7H1495v7H1497v-7H1499v7H1501v-7H1503v7H1505v-7H1507v7H1509v-7H1511v7H1513v-7H1515v7H1517v-7H1519v7H1521v-7H1523v7H1525v-7H1527v7H1529v-7H1531v7H1533v-7H1535v7H1537v-7H1539v7H1541v-7H1543v7H1545v-7H1547v7H1549v-7H1551v7H1553v-7H1555v7H1557v-7H1559v7H1561v-7H1563v7H1565v-7H1567v7H1569v-7H1571v7H1573v-7H1575v7H1577v-7H1579v7H1581v-7H1583v7H1585v-7H1587v7H1589v-7H1591v7H1593v-7H1595v7H1597v-7H1599v7H1601v-7H1603v7H1605v-7H1607v7H1609v-7H1611v7H1613v-7H1615v7H1617v-7H1619v7H1621v-7H1623v7H1625v-7H1627v7H1629v-7H1631v7H1633v-7H1635v7H1637v-7H1639v7H1641v-7H1643v7H1645v-7H1647v7H1649v-7H1651v7H1653v-7H1655v7H1657v-7H1659v7H1661v-7H1663v7H1665v-7H1667v7H1669v-7H1671v7H1673v-7H1675v7H1677v-7H1679v7H1681v-7H1683v7H1685v-7H1687v7H1689v-7H1691v7H1693v-7H1695v7H1697v-7H1699v7H1701v-7H1703v7H1705v-7H1707v7H1709v-7H1711v7H1713v-7H1715v7H1717v-7H1719v7H1721v-7H1723v7H1725v-7H1727v7H1729v-7H1731v7H1733v-7H1735v7H1737v-7H1739v7H1741v-7H1743v7H1745v-7H1747v7H1749v-7H1751v7H1753v-7H1755v7H1757v-7H1759v7H1761v-7H1763v7H1765v-7H1767v7H1769v-7H1771v7H1773v-7H1775v7H1777v-7H1779v7H1781v-7H1783v7H1785v-7H1787v7H1789v-7H1791v7H1793v-7H1795v7H1797v-7H1799v7H1801v-7H1803v7H1805v-7H1807v7H1809v-7H1811v7H1813v-7H1815v7H1817v-7H1819v7H1821v-7H1823v7H1825v-7H1827v7H1829v-7H1831v7H1833v-7H1835v7H1837v-7H1839v7H1841v-7H1843v7H1845v-7H1847v7H1849v-7H1851v7H1853v-7H1855v7H1857v-7H1859v7H1861v-7H1863v7H1865v-7H1867v7H1869v-7H1871v7H1873v-7H1875v7H1877v-7H1879v7H1881v-7H1883v7H1885v-7H1887v7H1889v-7H1891v7H1893v-7H1895v7H1897v-7H1899v7H1901v-7H1903v7H1905v-7H1907v7H1909v-7H1911v7H1913v-7H1915v7H1917v-7H1919v7H1921v-7H1923v7H1925v-7H1927v7H1929v-7H1931v7H1933v-7H1935v7H1937v-7H1939v7H1941v-7H1943v7H1945v-7H1947v7H1949v-7H1951v7H1953v-7H1955v7H1957v-7H1959v7H1961v-7H1963v7H1965v-7H1967v7H1969v-7H1971v7H1973v-7H1975v7H1977v-7H1979v7H1981v-7H1983v7H1985v-7H1987v7H1989v-7H1991v7H1993v-7H1995v7H1997v-7H1999v7H2001v-7H2003v7H2005v-7H2007v7H2009v-7H2011v7H2013v-7H2015v7H2017v-7H2019v7H2021v-7H2023v7H2025v-7H2027v7H2029v-7H2031v7H2033v-7H2035v7H2037v-7H2039v7H2041v-7H2043v7H2045v-7H2047v7H2049v-7H2051v7H2053v-7H2055v7H2057v-7H2059v7H2061v-7H2063v7H2065v-7H2067v7H2069v-7H2071v7H2073v-7H2075v7H2077v-7H2079v7H2081v-7H2083v7H2085v-7H2087v7H2089v-7H2091v7H2093v-7H2095v7H2097v-7H2099v7H2101v-7H2103v7H2105v-7H2107v7H2109v-7H2111v7H2113v-7H2115v7H2117v-7H2119v7H2121v-7H2123v7H2125v-7H2127v7H2129v-7H2131v7H2133v-7H2135v7H2137v-7H2139v7H2141v-7H2143v7H2145v-7H2147v7H2149v-7H2151v7H2153v-7H2155v7H2157v-7H2159v7H2161v-7H2163v7H2165v-7H2167v7H2169v-7H2171v7H2173v-7H2175v7H2177v-7H2179v7H2181v-7H2183v7H2185v-7H2187v7H2189v-7H2191v7H2193v-7H2195v7H2197v-7H2199v7H2201v-7H2203v7H2205v-7H2207v7H2209v-7H2211v7H2213v-7H2215v7H2217v-7H2219v7H2221v-7H2223v7H2225v-7H2227v7H2229v-7H2231v7H2233v-7H2235v7H2237v-7H2239v7H2241v-7H2243v7H2245v-7H2247v7H2249v-7H2251v7H2253v-7H2255v7H2257v-7H2259v7H2261v-7H2263v7H2265v-7H2267v7H2269v-7H2271v7H2273v-7H2275v7H2277v-7H2279v7H2281v-7H2283v7H2285v-7H2287v7H2289v-7H2291v7H2293v-7H2295v7H2297v-7H2299v7H2301v-7H2303v7H2305v-7H2307v7H2309v-7H2311v7H2313v-7H2315v7H2317v-7H2319v7H2321v-7H2323v7H2325v-7H2327v7H2329v-7H2331v7H2333v-7H2335v7H2337v-7H2339v7H2341v-7H2343v7H2345v-7H2347v7H2349v-7H2351v7H2353v-7H2355v7H2357v-7H2359v7H2361v-7H2363v7H2365v-7H2367v7H2369v-7H2371v7H2373v-7H2375v7H2377v-7H2379v7H2381v-7H2383v7H2385v-7H2387v7H2389v-7H2391v7H2393v-7H2395v7H2397v-7H2399v7H2401v-7H2403v7H2405v-7H2407v7H2409v-7H2411v7H2413v-7H2415v7H2417v-7H2419v7H2421v-7H2423v7H2425v-7H2427v7H2429v-7H2431v7H2433v-7H2435v7H2437v-7H2439v7H2441v-7H2443v7H2445v-7H2447v7H2449v-7H2451v7H2453v-7H2455v7H2457v-7H2459v7H2461v-7H2463v7H2465v-7H2467v7H2469v-7H2471v7H2473v-7H2475v7H2477v-7H2479v7H2481v-7H2483v7H2485v-7H2487v7H2489v-7H2491v7H2493v-7H2495v7H2497v-7H2499v7H2501v-7H2503v7H2505v-7H2507v7H2509v-7H2511v7H2513v-7H2515v7H2517v-7H2519v7H2521v-7H2523v7H2525v-7H2527v7H2529v-7H2531v7H2533v-7H2535v7H2537v-7H2539v7H2541v-7H2543v7H2545v-7H2547v7H2549v-7H2551v7H2553v-7H2555v7H2557v-7H2559v7H2561v-7H2563v7H2565v-7H2567v7H2569v-7H2571v7H2573v-7H2575v7H2577v-7H2579v7H2581v-7H2583v7H2585v-7H2587v7H2589v-7H2591v7H2593v-7H2595v7H2597v-7H2599v7H2601v-7H2603v7H2605v-7H2607v7H2609v-7H2611v7H2613v-7H2615v7H2617v-7H2619v7H2621v-7H2623v7H2625v-7H2627v7H2629v-7H2631v7H2633v-7H2635v7H2637v-7H2639v7H2641v-7H2643v7H2645v-7H2647v7H2649v-7H2651v7H2653v-7H2655v7H2657v-7H2659v7H2661v-7H2663v7H2665v-7H2667v7H2669v-7H2671v7H2673v-7H2675v7H2677v-7H2679v7H2681v-7H2683v7H2685v-7H2687v7H2689v-7H2691v7H2693v-7H2695v7H2697v-7H2699v7H2701v-7H2703v7H2705v-7H2707v7H2709v-7H2711v7H2713v-7H2715v7H2717v-7H2719v7H2721v-7H2723v7H2725v-7H2727v7H2729v-7H2731v7H2733v-7H2735v7H2737v-7H2739v7H2741v-7H2743v7H2745v-7H2747v7H2749v-7H2751v7H2753v-7H2755v7H2757v-7H2759v7H2761v-7H2763v7H2765v-7H2767v7H2769v-7H2771v7H2773v-7H2775v7H2777v-7H2779v7H2781v-7H2783v7H2785v-7H2787v7H2789v-7H2791v7H2793v-7H2795v7H2797v-7H2799v7H2801v-7H2803v7H2805v-7H2807v7H2809v-7H2811v7H2813v-7H2815v7H2817v-7H2819v7H2821v-7H2823v7H2825v-7H2827v7H2829v-7H2831v7H2833v-7H2835v7H2837v-7H2839v7H2841v-7H2843v7H2845v-7H2847v7H2849v-7H2851v7H2853v-7H2855v7H2857v-7H2859v7H2861v-7H2863v7H2865v-7H2867v7H2869v-7H2871v7H2873v-7H2875v7H2877v-7H2879v7H2881v-7H2883v7H2885v-7H2887v7H2889v-7H2891v7H2893v-7H2895v7H2897v-7H2899v7H2901v-7H2903v7H2905v-7H2907v7H2909v-7H2911v7H2913v-7H2915v7H2917v-7H2919v7H2921v-7H2923v7H2925v-7H2927v7H2929v-7H2931v7H2933v-7H2935v7H2937v-7H2939v7H2941v-7H2943v7H2945v-7H2947v7H2949v-7H2951v7H2953v-7H2955v7H2957v-7H2959v7H2961v-7H2963v7H2965v-7H2967v7H2969v-7H2971v7H2973v-7H2975v7H2977v-7H2979v7H2981v-7H2983v7H2985v-7H2987v7H2989v-7H2991v7H2993v-7H2995v7H2997v-7H2999v7H3001v-7H3003v7H3005v-7H3007v7H3009v-7H3011v7H3013v-7H3015v7H3017v-7H3019v7H3021v-7H3023v7H3025v-7H3027v7H3029v-7H3031v7H3033v-7H3035v7H3037v-7H3039v7H3041v-7H3043v7H3045v-7H3047v7H3049v-7H3051v7H3053v-7H3055v7H3057v-7H3059v7H3061v-7H3063v7H3065v-7H3067v7H3069v-7H3071v7H3073v-7H3075v7H3077v-7H3079v7H3081v-7H3083v7H3085v-7H3087v7H3089v-7H3091v7H3093v-7H3095v7H3097v-7H3099v7H3101v-7H3103v7H3105v-7H3107v7H3109v-7H3111v7H3113v-7H3115v7H3117v-7H3119v7H3121v-7H3123v7H3125v-7H3127v7H3129v-7H3131v7H3133v-7H3135v7H3137v-7H3139v7H3141v-7H3143v7H3145v-7H3147v7H3149v-7H3151v7H3153v-7H3155v7H3157v-7H3159v7H3161v-7H3163v7H3165v-7H3167v7H3169v-7H3171v7H3173v-7H3175v7H3177v-7H3179v7H3181v-7H3183v7H3185v-7H3187v7H3189v-7H3191v7H3193v-7H3195v7H3197v-7H3199v7H3201v-7H3203v7H3205v-7H3207v7H3209v-7H3211v7H3213v-7H3215v7H3217v-7H3219v7H3221v-7H3223v7H3225v-7H3227v7H3229v-7H3231v7H3233v-7H3235v7H3237v-7H3239v7H3241v-7H3243v7H3245v-7H3247v7H3249v-7H3251v7H3253v-7H3255v7H3257v-7H3259v7H3261v-7H3263v7H3265v-7H3267v7H3269v-7H3271v7H3273v-7H3275v7H3277v-7H3279v7H3281v-7H3283v7H3285v-7H3287v7H3289v-7H3291v7H3293v-7H3295v7H3297v-7H3299v7H3301v-7H3303v7H3305v-7H3307v7H3309v-7H3311v7H3313v-7H3315v7H3317v-7H3319v7H3321v-7H3323v7H3325v-7H3327v7H3329v-7H3331v7H3333v-7H3335v7H3337v-7H3339v7H3341v-7H3343v7H3345v-7H3347v7H3349v-7H3351v7H3353v-7H3355v7H3357v-7H3359v7H3361v-7H3363v7H3365v-7H3367v7H3369v-7H3
```

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
CAMELLIA128-SHA256	RSA	RSA	SHA256	Camellia(128)	MEDIUM
CAMELLIA256-SHA256	RSA	RSA	SHA256	Camellia(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ARIA128-GCM-SHA256	RSA	RSA	AEAD	ARIAGCM(128)	MEDIUM
ARIA256-GCM-SHA384	RSA	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-ARIA128-GCM-SHA256	ECDH	RSA	AEAD	ARIAGCM(128)	MEDIUM
ECDHE-RSA-ARIA256-GCM-SHA384	ECDH	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-CAMELLIA128-SHA256	ECDH	RSA	SHA256	Camellia(128)	MEDIUM
ECDHE-RSA-CAMELLIA256-SHA384	ECDH	RSA	SHA384	Camellia(256)	HIGH
AES128-CCM	RSA	RSA	AEAD	AESCCM(128)	MEDIUM
AES256-CCM	RSA	RSA	AEAD	AESCCM(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					



1 SSL Session Caching Information

port 8089/tcp over SSL

QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -

Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 8089/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 8089/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
AES256-SHA256	RSA		2048	no	110	low
AES128-SHA256	RSA		2048	no	110	low
AES256-CCM	RSA		2048	no	110	low
AES128-CCM	RSA		2048	no	110	low
ARIA256-GCM-SHA384	RSA		2048	no	110	low
ARIA128-GCM-SHA256	RSA		2048	no	110	low
CAMELLIA256-SHA256	RSA		2048	no	110	low

AES256-GCM-SHA384	RSA	2048	no	110	low
AES128-GCM-SHA256	RSA	2048	no	110	low
CAMELLIA256-SHA	RSA	2048	no	110	low
CAMELLIA128-SHA	RSA	2048	no	110	low
AES256-SHA	RSA	2048	no	110	low
AES128-SHA	RSA	2048	no	110	low
CAMELLIA128-SHA256	RSA	2048	no	110	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE x25519	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE x448	448	yes	224	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE x25519	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE x448	448	yes	224	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE x25519	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE x448	448	yes	224	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE x25519	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE x448	448	yes	224	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-ARIA256-GCM-SHA384	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE x25519	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE x448	448	yes	224	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-ARIA128-GCM-SHA256	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA384	ECDHE x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA384	ECDHE x448	448	yes	224	low
ECDHE-RSA-AES256-SHA384	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA384	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE x448	448	yes	224	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA256-SHA384	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA256	ECDHE x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA256	ECDHE x448	448	yes	224	low
ECDHE-RSA-AES128-SHA256	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA256	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE x25519	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE x448	448	yes	224	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE secp384r1	384	yes	192	low
ECDHE-RSA-CAMELLIA128-SHA256	ECDHE secp521r1	521	yes	260	low
ECDHE-RSA-AES256-SHA	ECDHE x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE x448	448	yes	224	low

ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 8089/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no

Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no



1 Secure Sockets Layer (SSL) Certificate Transparency Information

port 8089/tcp over SSL

QID: 38718
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.anla.gov.co, O=U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA, ST=Distrito Capital de Bogot, C=CO			
Certificate	no	(unknown)	(unknown)	d809553b944f7affc816196f9 44f85abb0f8fc5e8755260f15 d12e72bb454b14	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	af67883b57b04edd8fa6d97ef 62ea8eb810ac77160f0245e55 d60c2fe785873a	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	acab30706cebec8431f413d2f 4915f111e422443b1f2a68c4f 3c2b3ba71e02c3	Thu 01 Jan 1970 12:00:00 AM GMT



QID: 38994
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

It reports complete list of all host-supported PQC key-exchange algorithms along with full handshake details.
If server hosts any service

over TLS1.3, then a probe is sent to validate if the service supports following PQC key exchange algorithms.
MLKEM512
MLKEM768
MLKEM1024
X25519MLKEM768
SecP256r1MLKEM768
SecP384r1MLKEM1024

Field
Description
Cipher name
Cipher used
Protocol
TLS
version
Key-exchange
Negotiated PQC KEX
Authentication
Signature algorithm
MAC
Message authentication code
Encryption + key
strength
Encryption mode and key size
NIST security strength
Security strength (NIST equivalent)

Reference: <https://csrc.nist.gov/groups/ST/post-quantum-crypto/evaluation-criteria.html>

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	STRENGTH
TLS13-AES-256-GCM-SHA384	X25519MLKEM768	RSA-PSS	AEAD	AESGCM(256)	192-bit



1 Reports Signature Algorithm used in Post Quantum Cryptographic(PQC) detection using QID 38994

port 8089/tcp over SSL

QID: 38995
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

If server hosts any service over TLS1.3, then a probe is sent to validate if the service supports PQC key exchange algorithms as part of QID38994.

This QID reports Signature Algorithm used by the service for Post Quantum Cryptographic(PQC) SSL handshake using QID 38994.

It

reports server's preferred PQC signature algorithm.
This QID is planned for future deprecation.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:



1 TLS Secure Renegotiation Extension Support Information

port 8089/tcp over SSL

QID: 42350
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tie renegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 8089/tcp over SSL

QID: 48340
Category: Information gathering
Associated CVEs: -
Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
Bugtraq ID: -
Service Modified: 04/13/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported

**1 SSL Certificate - Information**

port 8089/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	b2:f8:3d:72:1f:f3:a7:29:60:a2:df:c3:eb:8c:4e:fe

(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(0)SUBJECT NAME	
countryName	CO
stateOrProvinceName	Distrito Capital de BogotáC3A1
organizationName	U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA
commonName	*.anla.gov.co
(0)Valid From	Oct 22 00:00:00 2025 GMT
(0)Valid Till	Nov 3 23:59:59 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c5:22:80:6e:68:2e:0a:69:6c:67:0c:b8:ee:74:
(0)	e6:56:64:4b:b8:7c:61:47:27:e3:6d:60:a6:34:1e:
(0)	77:20:80:97:2e:ef:ac:2a:8c:52:08:59:9b:33:1e:
(0)	46:70:61:83:8e:1a:85:af:55:76:33:a3:94:c1:04:
(0)	e3:2c:f3:01:07:35:c1:4a:dc:48:47:42:2f:ae:f1:
(0)	fd:b7:49:e5:ff:21:ba:47:cb:bf:1e:4d:13:d3:32:
(0)	17:73:33:65:22:03:ee:2d:36:f2:bc:5a:a5:7d:ad:
(0)	03:01:c2:c0:fe:95:9e:af:81:95:bb:43:59:95:4a:
(0)	bf:82:31:de:e6:1b:43:f4:11:c0:36:be:2c:00:fc:
(0)	2f:97:4b:bb:78:87:61:6e:29:1a:91:8b:a6:2d:f6:
(0)	27:75:93:c2:46:8d:84:cf:b6:8a:69:98:4d:2d:b3:
(0)	4c:1d:44:ea:f6:a4:f9:00:5b:c8:8a:ed:77:66:b3:
(0)	ce:b1:87:b7:e7:52:95:da:e2:08:0d:bb:03:78:02:
(0)	17:46:ce:46:e7:83:f1:1d:ba:47:a3:e2:0e:e3:7b:
(0)	dc:ff:47:79:09:ff:a4:5a:2d:58:4c:d4:1c:24:af:
(0)	a1:aa:ed:50:96:8e:9c:e5:7a:a2:ba:91:53:30:4c:
(0)	42:04:c6:39:7b:c1:f3:88:68:7b:6f:5a:8b:1d:ef:
(0)	5c:5f
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(0)X509v3 Subject Key Identifier	3A:B2:87:43:6F:E2:96:F3:ED:40:44:B2:5F:8C:7E:8B:8F:2C:CD:44
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.1.3.4
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.2
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
(0)	OCSP - URI:http://ocsp.sectigo.com
(0)X509v3 Subject Alternative Name	DNS:*.anla.gov.co, DNS:anla.gov.co
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:

(0)	B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14
(0)	Timestamp : Oct 22 21:05:01.112 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:DB:DF:24:6B:4B:B4:A3:AF:88:F0:38:
(0)	D1:3F:21:84:EF:C7:FF:E9:37:FB:FE:CD:B6:CA:04:EF:
(0)	45:22:C8:5B:32:02:21:00:F3:94:94:8C:3F:DA:C9:34:
(0)	51:AE:9A:73:07:1B:37:36:DC:28:62:98:D7:5C:66:52:
(0)	98:71:17:EA:46:23:10:97
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AF:67:88:3B:57:B0:4E:DD:8F:A6:D9:7E:F6:2E:A8:EB:
(0)	81:0A:C7:71:60:F0:24:5E:55:D6:0C:2F:E7:85:87:3A
(0)	Timestamp : Oct 22 21:05:01.223 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:D2:A5:92:31:F6:F8:92:C8:0D:45:20:
(0)	A9:43:B4:3D:09:ED:63:29:FE:6C:BF:13:91:72:85:72:
(0)	ED:AF:05:9C:32:02:20:08:8A:F2:6D:EA:45:68:1A:22:
(0)	08:F4:76:CA:54:F5:B5:75:78:5E:A5:3B:2B:94:42:20:
(0)	03:D1:89:A3:78:FC:78
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AC:AB:30:70:6C:EB:EC:84:31:F4:13:D2:F4:91:5F:11:
(0)	1E:42:24:43:B1:F2:A6:8C:4F:3C:2B:3B:A7:1E:02:C3
(0)	Timestamp : Oct 22 21:05:00.999 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:7A:D5:12:14:07:82:C9:A8:23:A7:95:43:
(0)	83:2B:93:B8:98:74:39:EA:8B:81:EE:6B:D9:1C:CB:DB:
(0)	50:74:D2:BA:02:21:00:C0:5F:F6:05:5B:47:AB:76:2E:
(0)	57:C7:FB:81:9B:91:F0:94:D6:15:89:F5:92:BF:31:F6:
(0)	02:CB:61:FB:61:95:9F
(0)Signature	(384 octets)
(0)	6f:c0:09:87:ec:ea:a5:4c:65:e0:96:7f:ee:cd:75:35
(0)	51:57:14:d5:af:5b:ed:55:e5:c4:27:67:93:7e:af:0a
(0)	ad:d2:a5:b9:86:c9:52:60:fc:8e:01:3c:33:bc:68:e2
(0)	7e:29:00:f6:4b:55:d6:1b:1e:a5:3e:e7:65:02:a5:c5
(0)	9d:6a:a2:d2:7e:68:e5:19:af:6d:81:db:29:c8:c8:6b
(0)	20:fa:eb:0b:70:20:be:bc:bb:89:48:ae:d4:d1:a8:ae
(0)	5c:01:be:87:43:5a:c6:43:b6:4a:de:24:a3:02:3b:67
(0)	d4:03:ab:90:d1:68:e0:7f:c7:f5:7d:15:2c:c7:bd:bd
(0)	35:33:ba:a3:1f:c6:a9:57:aa:a6:c7:ad:98:be:2a:8f
(0)	cb:c2:2e:1e:7f:7c:0f:e4:f0:a0:61:5a:24:66:24:ae
(0)	19:1c:8b:9f:3a:bc:a1:b4:47:71:63:43:2c:01:59:7c
(0)	9a:6a:88:aa:5f:f4:91:4a:7f:28:08:7b:61:52:4b:da
(0)	20:a9:e7:0e:35:a9:87:c5:1c:74:86:d2:56:7a:87:eb
(0)	03:73:4c:44:6e:c8:fd:b0:d0:f6:1f:d0:69:82:ab:57
(0)	d4:6d:2c:d7:7b:5a:60:ce:20:2a:6a:1f:0f:43:2a:79
(0)	f0:74:86:d8:6c:dc:86:a5:ca:98:d8:ae:38:79:36:38
(0)	2d:a1:02:36:5d:c2:04:3f:1a:f5:ea:00:99:b7:78:0c
(0)	fe:36:07:9b:5d:21:f9:14:65:37:d8:d8:e5:fd:ee:1a
(0)	c0:c3:a8:d7:0d:d5:a8:d2:0b:da:c5:c8:39:03:52:1d
(0)	84:ec:2d:67:f9:c1:7d:79:56:0b:8d:b4:b8:74:30:63
(0)	4c:02:98:d1:6a:0b:76:e9:72:2d:90:78:ac:96:88:a0

(0)	64:04:46:cd:3f:75:64:2a:79:14:a5:88:48:6d:ed:a2
(0)	e5:8b:eb:10:91:9c:05:2a:32:20:d3:d5:a7:d8:16:1d
(0)	4f:c1:91:ed:6d:93:a3:00:8d:b8:26:d0:cc:47:cf:57
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(1)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(1)Valid From	Mar 22 00:00:00 2021 GMT
(1)Valid Till	Mar 21 23:59:59 2036 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(3072 bit)
(1)	RSA Public-Key: (3072 bit)
(1)	Modulus:
(1)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(1)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(1)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(1)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(1)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(1)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(1)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(1)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(1)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(1)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(1)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(1)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(1)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(1)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(1)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(1)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(1)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(1)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(1)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(1)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(1)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(1)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(1)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(1)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(1)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(1)	36:d7:77:f5:91:27:08:66:7b:4d
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(1)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0

(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	Policy: 2.23.140.1.2.2
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(1)	OCSP - URI:http://ocsp.sectigo.com
(1)Signature	(512 octets)
(1)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(1)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(1)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(1)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(1)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(1)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(1)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(1)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(1)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(1)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(1)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(1)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(1)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(1)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(1)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(1)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(1)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(1)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(1)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(1)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(1)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(1)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(1)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(1)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(1)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(1)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(1)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(1)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(1)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(1)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(1)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(1)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(2)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46

(2)Valid From	Mar 22 00:00:00 2021 GMT
(2)Valid Till	Jan 18 23:59:59 2038 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(2)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(2)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(2)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(2)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(2)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(2)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(2)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(2)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(2)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(2)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(2)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(2)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(2)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(2)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(2)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(2)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(2)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(2)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(2)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(2)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(2)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(2)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(2)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(2)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(2)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(2)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(2)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(2)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(2)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(2)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(2)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(2)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(2)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(2)	7c:6d:cf
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(2)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com

(2)Signature	(512 octets)
(2)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(2)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(2)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(2)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(2)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(2)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(2)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(2)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(2)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(2)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(2)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(2)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(2)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(2)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(2)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(2)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(2)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(2)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(2)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(2)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(2)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(2)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(2)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(2)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(2)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(2)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(2)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(2)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(2)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(2)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(2)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(2)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(3)CERTIFICATE 3	
(3)Version	3 (0x2)
(3)Serial Number	01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d
(3)Signature Algorithm	sha384WithRSAEncryption
(3)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)SUBJECT NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)Valid From	Feb 1 00:00:00 2010 GMT
(3)Valid Till	Jan 18 23:59:59 2038 GMT
(3)Public Key Algorithm	rsaEncryption
(3)RSA Public Key	(4096 bit)
(3)	RSA Public-Key: (4096 bit)
(3)	Modulus:

(3)	00:80:12:65:17:36:0e:c3:db:08:b3:d0:ac:57:0d:
(3)	76:ed:cd:27:d3:4c:ad:50:83:61:e2:aa:20:4d:09:
(3)	2d:64:09:dc:ce:89:9f:cc:3d:a9:ec:f6:cf:c1:dc:
(3)	f1:d3:b1:d6:7b:37:28:11:2b:47:da:39:c6:bc:3a:
(3)	19:b4:5f:a6:bd:7d:9d:a3:63:42:b6:76:f2:a9:3b:
(3)	2b:91:f8:e2:6f:d0:ec:16:20:90:09:3e:e2:e8:74:
(3)	c9:18:b4:91:d4:62:64:db:7f:a3:06:f1:88:18:6a:
(3)	90:22:3c:bc:fe:13:f0:87:14:7b:f6:e4:1f:8e:d4:
(3)	e4:51:c6:11:67:46:08:51:cb:86:14:54:3f:bc:33:
(3)	fe:7e:6c:9c:ff:16:9d:18:bd:51:8e:35:a6:a7:66:
(3)	c8:72:67:db:21:66:b1:d4:9b:78:03:c0:50:3a:e8:
(3)	cc:f0:dc:bc:9e:4c:fe:af:05:96:35:1f:57:5a:b7:
(3)	ff:ce:f9:3d:b7:2c:b6:f6:54:dd:c8:e7:12:3a:4d:
(3)	ae:4c:8a:b7:5c:9a:b4:b7:20:3d:ca:7f:22:34:ae:
(3)	7e:3b:68:66:01:44:e7:01:4e:46:53:9b:33:60:f7:
(3)	94:be:53:37:90:73:43:f3:32:c3:53:ef:db:aa:fe:
(3)	74:4e:69:c7:6b:8c:60:93:de:c4:c7:0c:df:e1:32:
(3)	ae:cc:93:3b:51:78:95:67:8b:ee:3d:56:fe:0c:d0:
(3)	69:0f:1b:0f:f3:25:26:6b:33:6d:f7:6e:47:fa:73:
(3)	43:e5:7e:0e:a5:66:b1:29:7c:32:84:63:55:89:c4:
(3)	0d:c1:93:54:30:19:13:ac:d3:7d:37:a7:eb:5d:3a:
(3)	6c:35:5c:db:41:d7:12:da:a9:49:0b:df:d8:80:8a:
(3)	09:93:62:8e:b5:66:cf:25:88:cd:84:b8:b1:3f:a4:
(3)	39:0f:d9:02:9e:eb:12:4c:95:7c:f3:6b:05:a9:5e:
(3)	16:83:cc:b8:67:e2:e8:13:9d:cc:5b:82:d3:4c:b3:
(3)	ed:5b:ff:de:e5:73:ac:23:3b:2d:00:bf:35:55:74:
(3)	09:49:d8:49:58:1a:7f:92:36:e6:51:92:0e:f3:26:
(3)	7d:1c:4d:17:bc:c9:ec:43:26:d0:bf:41:5f:40:a9:
(3)	44:44:f4:99:e7:57:87:9e:50:1f:57:54:a8:3e:fd:
(3)	74:63:2f:b1:50:65:09:e6:58:42:2e:43:1a:4c:b4:
(3)	f0:25:47:59:fa:04:1e:93:d4:26:46:4a:50:81:b2:
(3)	de:be:78:b7:fc:67:15:e1:c9:57:84:1e:0f:63:d6:
(3)	e9:62:ba:d6:5f:55:2e:ea:5c:c6:28:08:04:25:39:
(3)	b8:0e:2b:a9:f2:4c:97:1c:07:3f:0d:52:f5:ed:ef:
(3)	2f:82:0f
(3)	Exponent: 65537 (0x10001)
(3)X509v3 EXTENSIONS	
(3)X509v3 Subject Key Identifier	53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(3)X509v3 Key Usage	critical
(3)	Certificate Sign, CRL Sign
(3)X509v3 Basic Constraints	critical
(3)	CA:TRUE
(3)Signature	(512 octets)
(3)	5c:d4:7c:0d:cf:f7:01:7d:41:99:65:0c:73:c5:52:9f
(3)	cb:f8:cf:99:06:7f:1b:da:43:15:9f:9e:02:55:57:96
(3)	14:f1:52:3c:27:87:94:28:ed:1f:3a:01:37:a2:76:fc
(3)	53:50:c0:84:9b:c6:6b:4e:ba:8c:21:4f:a2:8e:55:62
(3)	91:f3:69:15:d8:bc:88:e3:c4:aa:0b:fd:ef:a8:e9:4b
(3)	55:2a:06:20:6d:55:78:29:19:ee:5f:30:5c:4b:24:11
(3)	55:ff:24:9a:6e:5e:2a:2b:ee:0b:4d:9f:7f:f7:01:38
(3)	94:14:95:43:07:09:fb:60:a9:ee:1c:ab:12:8c:a0:9a
(3)	5e:a7:98:6a:59:6d:8b:3f:08:fb:c8:d1:45:af:18:15
(3)	64:90:12:0f:73:28:2e:c5:e2:24:4e:fc:58:ec:f0:f4
(3)	45:fe:22:b3:eb:2f:8e:d2:d9:45:61:05:c1:97:6f:a8
(3)	76:72:8f:8b:8c:36:af:bf:0d:05:ce:71:8d:e6:a6:6f

(3)	1f:6c:a6:71:62:c5:d8:d0:83:72:0c:f1:67:11:89:0c
(3)	9c:13:4c:72:34:df:bc:d5:71:df:aa:71:dd:e1:b9:6c
(3)	8c:3c:12:5d:65:da:bd:57:12:b6:43:6b:ff:e5:de:4d
(3)	66:11:51:cf:99:ae:ec:17:b6:e8:71:91:8c:de:49:fe
(3)	dd:35:71:a2:15:27:94:1c:cf:61:e3:26:bb:6f:a3:67
(3)	25:21:5d:e6:dd:1d:0b:2e:68:1b:3b:82:af:ec:83:67
(3)	85:d4:98:51:74:b1:b9:99:80:89:ff:7f:78:19:5c:79
(3)	4a:60:2e:92:40:ae:4c:37:2a:2c:c9:c7:62:c8:0e:5d
(3)	f7:36:5b:ca:e0:25:25:01:b4:dd:1a:07:9c:77:00:3f
(3)	d0:dc:d5:ec:3d:d4:fa:bb:3f:cc:85:d6:6f:7f:a9:2d
(3)	df:b9:02:f7:f5:97:9a:b5:35:da:c3:67:b0:87:4a:a9
(3)	28:9e:23:8e:ff:5c:27:6b:e1:b0:4f:f3:07:ee:00:2e
(3)	d4:59:87:cb:52:41:95:ea:f4:47:d7:ee:64:41:55:7c
(3)	8d:59:02:95:dd:62:9d:c2:b9:ee:5a:28:74:84:a5:9b
(3)	b7:90:c7:0c:07:df:f5:89:36:74:32:d6:28:c1:b0:b0
(3)	0b:e0:9c:4c:c3:1c:d6:fc:e3:69:b5:47:46:81:2f:a2
(3)	82:ab:d3:63:44:70:c4:8d:ff:2d:33:ba:ad:8f:7b:b5
(3)	70:88:ae:3e:19:cf:40:28:d8:fc:c8:90:bb:5d:99:22
(3)	f5:52:e6:58:c5:1f:88:31:43:ee:88:1d:d7:c6:8e:3c
(3)	43:6a:1d:a7:18:de:7d:3d:16:f1:62:f9:ca:90:a8:fd
(4)CERTIFICATE 4	
(4)Version	3 (0x2)
(4)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(4)Signature Algorithm	sha384WithRSAEncryption
(4)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(4)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(4)Valid From	Mar 22 00:00:00 2021 GMT
(4)Valid Till	Jan 18 23:59:59 2038 GMT
(4)Public Key Algorithm	rsaEncryption
(4)RSA Public Key	(4096 bit)
(4)	RSA Public-Key: (4096 bit)
(4)	Modulus:
(4)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(4)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(4)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(4)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(4)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(4)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(4)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(4)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(4)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(4)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(4)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(4)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(4)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(4)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(4)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:

(4)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(4)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(4)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(4)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(4)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(4)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(4)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(4)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(4)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(4)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(4)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(4)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(4)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(4)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(4)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(4)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(4)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(4)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(4)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(4)	7c:6d:cf
(4)	Exponent: 65537 (0x10001)
(4)X509v3 EXTENSIONS	
(4)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(4)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(4)X509v3 Key Usage	critical
(4)	Digital Signature, Certificate Sign, CRL Sign
(4)X509v3 Basic Constraints	critical
(4)	CA:TRUE
(4)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(4)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(4)X509v3 CRL Distribution Points	
(4)	Full Name:
(4)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(4)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(4)Signature	(512 octets)
(4)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(4)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(4)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(4)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(4)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(4)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(4)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(4)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(4)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(4)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(4)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(4)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(4)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(4)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(4)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(4)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(4)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(4)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(4)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(4)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9

(4)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(4)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(4)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(4)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(4)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(4)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(4)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(4)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(4)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(4)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(4)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(4)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(5)CERTIFICATE 5	
(5)Version	3 (0x2)
(5)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(5)Signature Algorithm	sha384WithRSAEncryption
(5)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(5)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(5)Valid From	Mar 22 00:00:00 2021 GMT
(5)Valid Till	Mar 21 23:59:59 2036 GMT
(5)Public Key Algorithm	rsaEncryption
(5)RSA Public Key	(3072 bit)
(5)	RSA Public-Key: (3072 bit)
(5)	Modulus:
(5)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(5)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(5)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(5)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(5)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(5)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(5)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(5)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(5)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(5)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(5)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(5)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(5)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(5)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(5)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(5)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(5)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(5)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(5)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(5)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(5)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(5)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(5)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(5)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(5)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:

(5)	36:d7:77:f5:91:27:08:66:7b:4d
(5)	Exponent: 65537 (0x10001)
(5)X509v3 EXTENSIONS	
(5)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(5)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(5)X509v3 Key Usage	critical
(5)	Digital Signature, Certificate Sign, CRL Sign
(5)X509v3 Basic Constraints	critical
(5)	CA:TRUE, pathlen:0
(5)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(5)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(5)	Policy: 2.23.140.1.2.2
(5)X509v3 CRL Distribution Points	
(5)	Full Name:
(5)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(5)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(5)	OCSP - URI:http://ocsp.sectigo.com
(5)Signature	(512 octets)
(5)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(5)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(5)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(5)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(5)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(5)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(5)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(5)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(5)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(5)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(5)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(5)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(5)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(5)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(5)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(5)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(5)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(5)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(5)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(5)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(5)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(5)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(5)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(5)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(5)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(5)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(5)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(5)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(5)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(5)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(5)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(5)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c



1 Web Server Supports HTTP Request Pipelining

port 8089/tcp over SSL

QID: 86565

Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (<http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf>), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:172.40.123.5:8089

GET /Q_Evasive/ HTTP/1.1
Host:172.40.123.5:8089

HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:41:31 GMT
Content-Type: text/html
Content-Length: 2706
Last-Modified: Fri, 10 Apr 2026 18:57:21 GMT
Connection: keep-alive
ETag: "69d94811-a92"
Accept-Ranges: bytes

```
<!doctype html>
<html lang="es">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <title>Reporte PAI _E2_80_93 Frontend</title>
  <link rel="stylesheet" href="styles.css" />
</head>
<body>
  <header>
    <div class="brand">
```

```

    <svg viewBox="0 0 24 24" width="22" height="22" aria-hidden="true"><path fill="currentColor" d="M19 3H5a2 2 0 0 0 2 2v14a2 2 0 0 0 2 2h14a2 2 0 0 0 2 2v5a2 2 0 0 0 2 2Zm-7 14H7v-2h5v2Zm5-4H7v-2h10v2Zm0-4H7V7h10v2Z"/></svg>
    <span>Reporte PAI</span>
  </div>
</header>

<main>
  <h1 class="page-title">
    <svg viewBox="0 0 24 24" width="22" height="22" aria-hidden="true"><path fill="currentColor" d="M12 2a10 10 0 1 0 10 10A10.011 10.011 0 0 0 12 2Zm1 14h-2v-2h2Zm0-4h-2V6h2Z"/></svg>
    Validaci_C3_B3n de Documentos
  </h1>
  <p class="subtitle">Sube tu archivo y procesaremos autom_C3_A1ticamente el informe.</p>

  <section class="card">
    <h2>Archivo a procesar</h2>

    <div class="row">
      <label for="corte_mes">Corte de mes</label>
      <div class="input-inline">
        <input id="corte_mes" name="corte_mes" type="text"
          placeholder="YYYY-MM o YYYY-MM-DD o _E2_80_98marzo 2026 _E2_80_99" />
        <button id="btn-fill" type="button" title="Usar mes actual">_E2_9F_B2</button>
      </div>
      <small class="hint">Tip: usa <b>YYYY-MM</b> para corte mensual.</small>
    </div>

    <div id="dropzone" class="dropzone" tabindex="0" role="button" aria-label="Zona para arrastrar y soltar archivo">
      <div class="dz-inner">
        <svg viewBox="0 0 24 24" width="38" height="38" aria-hidden="true"><path fill="currentColor" d="M19 12v7H5v-7H3v7a2 2 0 0 0 2 2h14a2 2 0 0 0 2 2v-7Zm11 6.414 8.707 8.707 7.293 7.293 12 2.586l4.707 4.707-1.414 1.414L13 6.414V16h-2Z"/></svg>
        <p class="dz-title">Arrastra tu archivo aqu_C3_AD</p>
        <p class="dz-help">o haz clic para seleccionar</p>
        <p class="dz-note">Formato: XLSX (m_C3_A1x. 20MB)</p>
      </div>
      <input id="file" type="file" accept=".xlsx" aria-label="Seleccionar archivo" />
    </div>

    <div class="file-chip" id="file-chip" hidden>
      <span id="file-name"></span>
      <button id="btn-clear" type="button" aria-label="Quitar archivo">_C3_97</button>
    </div>

    <div class="actions">
      <button id="btn-process" type="button" disabled>Procesar documento</button>
    </div>

    <div id="status" class="status" role="status" aria-live="polite"></div>
    <div id="result" class="result"></div>
  </section>
</main>

<footer>
  <small>_C2_A9 Reporte PAI _E2_80_93 Frontend</small>
</footer>

<script src="app.js"></script>
</body>
</html>
HTTP/1.1 200 OK
Server: nginx/1.29.8
Date: Sat, 25 Apr 2026 02:41:31 GMT
Content-Type: text/html
Content-Length: 2706
Last-Modified: Fri, 10 Apr 2026 18:57:21 GMT
Connection: keep-alive
ETag: "69d94811-a92"
Accept-Ranges: bytes

<!doctype html>
<html lang="es">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <title>Reporte PAI _E2_80_93 Frontend</title>
  <link rel="stylesheet" href="styles.css" />
</head>

```

```

<body>
<header>
  <div class="brand">
    <svg viewBox="0 0 24 24" width="22" height="22" aria-hidden="true"><path fill="currentColor" d="M19 3H5a2 2 0 0 0-2 2v14a2 2 0 0 0 2 2h14a2 2 0 0 0 2-2V5a2 2 0 0 0-2-2Zm-7 14H7v-2h5v2Zm5-4H7v-2h10v2Zm0-4H7V7h10v2Z"/></svg>
    <span>Reporte PAI</span>
  </div>
</header>

<main>
  <h1 class="page-title">
    <svg viewBox="0 0 24 24" width="22" height="22" aria-hidden="true"><path fill="currentColor" d="M12 2a10 10 0 1 0 10 10A10.011 10.011 0 0 0 12 2Zm1 14h-2v-2h2Zm0-4h-2V6h2Z"/></svg>
    Validaci_C3_B3n de Documentos
  </h1>
  <p class="subtitle">Sube tu archivo y procesaremos autom_C3_A1ticamente el informe.</p>

  <section class="card">
    <h2>Archivo a procesar</h2>

    <div class="row">
      <label for="corte_mes">Corte de mes</label>
      <div class="input-inline">
        <input id="corte_mes" name="corte_mes" type="text"
          placeholder="YYYY-MM o YYYY-MM-DD o _E2_80_98marzo 2026_E2_80_99" />
        <button id="btn-fill" type="button" title="Usar mes actual">_E2_9F_B2</button>
      </div>
      <small class="hint">Tip: usa <b>YYYY-MM</b> para corte mensual.</small>
    </div>

    <div id="dropzone" class="dropzone" tabindex="0" role="button" aria-label="Zona para arrastrar y soltar archivo">
      <div class="dz-inner">
        <svg viewBox="0 0 24 24" width="38" height="38" aria-hidden="true"><path fill="currentColor" d="M19 12v7H5v-7H3v7a2 2 0 0 0 2 2h14a2 2 0 0 0 2-2v-7ZM11 6.414 8.707 8.707 7.293 7.293 12 2.586l4.707 4.707-1.414 1.414L13 6.414V16h-2Z"/></svg>
        <p class="dz-title">Arrastra tu archivo aqu_C3_AD</p>
        <p class="dz-help">o haz clic para seleccionar</p>
        <p class="dz-note">Formato: XLSX (m_C3_A1x. 20MB)</p>
      </div>
      <input id="file" type="file" accept=".xlsx" aria-label="Seleccionar archivo" />
    </div>

    <div class="file-chip" id="file-chip" hidden>
      <span id="file-name"></span>
      <button id="btn-clear" type="button" aria-label="Quitar archivo">_C3_97</button>
    </div>

    <div class="actions">
      <button id="btn-process" type="button" disabled>Procesar documento</button>
    </div>

    <div id="status" class="status" role="status" aria-live="polite"></div>
    <div id="result" class="result"></div>
  </section>
</main>

<footer>
  <small>_C2_A9 Reporte PAI _E2_80_93 Frontend</small>
</footer>

<script src="app.js"></script>
</body>
</html>

```



1 Default Web Page

port 8093/tcp over SSL

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8093
Connection: Keep-Alive

{"detail":"Not Found"}



1 Default Web Page (Follow HTTP Redirection)

port 8093/tcp over SSL

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8093
Connection: Keep-Alive

{"detail": "Not Found"}



1 SSL Server Information Retrieval

port 8093/tcp over SSL

QID: 38116
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH



1 SSL Session Caching Information

port 8093/tcp over SSL

QID: 38291
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/19/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 8093/tcp over SSL

QID: 38597
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 07/12/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 8093/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						

**1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties**

port 8093/tcp over SSL

QID: 38706
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no



1 Secure Sockets Layer (SSL) Certificate Transparency Information

port 8093/tcp over SSL

QID: 38718
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated Name	URL	ID	Time
Certificate #0	CN=*.anla.gov.co, O=U A E AUTORIDAD NACIONAL DE LICENCIAS			

Certificate	no	(unknown)	(unknown)	d809553b944f7affc816196f9 44f85abb0f8fc5e8755260f15 d12e72bb454b14	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	af67883b57b04edd8fa6d97ef 62ea8eb810ac77160f0245e55 d60c2fe785873a	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	acab30706cebec8431f413d2f 4915f111e422443b1f2a68c4f 3c2b3ba71e02c3	Thu 01 Jan 1970 12:00:00 AM GMT



1 Reports if server supports Post Quantum Cryptographic(PQC) Key Exchange Algorithm

port 8093/tcp over SSL

QID: 38994
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 01/05/2026
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

It reports complete list of all host-supported PQC key-exchange algorithms along with full handshake details.
If server hosts any service

over TLS1.3, then a probe is sent to validate if the service supports following PQC key exchange

algorithms.
 MLKEM512
 MLKEM768
 MLKEM1024
 X25519MLKEM768
 SecP256r1MLKEM768
 SecP384r1MLKEM1024

Field
 Description

 Cipher name
 Cipher used

 Protocol
 TLS
 version

 Key-exchange
 Negotiated PQC KEX

 Authentication
 Signature algorithm

 MAC
 Message authentication code

 Encryption + key

strength
Encryption mode and key size

NIST security strength
Security strength (NIST
equivalent)

Reference: <https://csrc.nist.gov/groups/ST/post-quantum-crypto/evaluation-criteria.html>

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	STRENGTH
TLS13-AES-256-GCM-SHA384	X25519MLKEM768	RSA-PSS	AEAD	AESGCM(256)	192-bit



1 Reports Signature Algorithm used in Post Quantum Cryptographic(PQC) detection using QID 38994

port 8093/tcp over SSL

QID: 38995
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

If server hosts any service over TLS1.3, then a probe is sent to validate if the service supports PQC key exchange algorithms as part of QID38994.

This QID reports Signature Algorithm used by the service for Post Quantum Cryptographic(PQC) SSL handshake using QID 38994.

It

reports server's preferred PQC signature algorithm.
This QID is planned for future deprecation.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Preferred PQC Signature Algorithm: RSA-PSS



1 TLS Secure Renegotiation Extension Support Information

port 8093/tcp over SSL

QID: 42350
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tier renegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 8093/tcp over SSL

QID: 48340

Category: Information gathering
Associated CVEs: -
Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
Bugtraq ID: -
Service Modified: 04/13/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 8093/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	b2:f8:3d:72:1f:f3:a7:29:60:a2:df:c3:eb:8c:4e:fe
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(0)SUBJECT NAME	
countryName	CO
stateOrProvinceName	Distrito Capital de BogotáC3A1
organizationName	U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA
commonName	*.anla.gov.co
(0)Valid From	Oct 22 00:00:00 2025 GMT
(0)Valid Till	Nov 3 23:59:59 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c5:22:80:6e:68:2e:0a:69:6c:67:0c:b8:ee:74:
(0)	e6:56:64:4b:b8:7c:61:47:27:e3:6d:60:a6:34:1e:
(0)	77:20:80:97:2e:ef:ac:2a:8c:52:08:59:9b:33:1e:
(0)	46:70:61:83:8e:1a:85:af:55:76:33:a3:94:c1:04:
(0)	e3:2c:f3:01:07:35:c1:4a:dc:48:47:42:2f:ae:f1:
(0)	fd:b7:49:e5:ff:21:ba:47:cb:bf:1e:4d:13:d3:32:
(0)	17:73:33:65:22:03:ee:2d:36:f2:bc:5a:a5:7d:ad:
(0)	03:01:c2:c0:fe:95:9e:af:81:95:bb:43:59:95:4a:
(0)	bf:82:31:de:e6:1b:43:f4:11:c0:36:be:2c:00:fc:
(0)	2f:97:4b:bb:78:87:61:6e:29:1a:91:8b:a6:2d:f6:
(0)	27:75:93:c2:46:8d:84:cf:b6:8a:69:98:4d:2d:b3:
(0)	4c:1d:44:ea:f6:a4:f9:00:5b:c8:8a:ed:77:66:b3:
(0)	ce:b1:87:b7:e7:52:95:da:e2:08:0d:bb:03:78:02:
(0)	17:46:ce:46:e7:83:f1:1d:ba:47:a3:e2:0e:e3:7b:
(0)	dc:ff:47:79:09:ff:a4:5a:2d:58:4c:d4:1c:24:af:
(0)	a1:aa:ed:50:96:8e:9c:e5:7a:a2:ba:91:53:30:4c:
(0)	42:04:c6:39:7b:c1:f3:88:68:7b:6f:5a:8b:1d:ef:
(0)	5c:5f
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(0)X509v3 Subject Key Identifier	3A:B2:87:43:6F:E2:96:F3:ED:40:44:B2:5F:8C:7E:8B:8F:2C:CD:44
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.1.3.4

(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.2
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI: http://crl.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crl
(0)Authority Information Access	CA Issuers - URI: http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
(0)	OCSP - URI: http://ocsp.sectigo.com
(0)X509v3 Subject Alternative Name	DNS:*.anla.gov.co, DNS:anla.gov.co
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:
(0)	B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14
(0)	Timestamp : Oct 22 21:05:01.112 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:DB:DF:24:6B:4B:B4:A3:AF:88:F0:38:
(0)	D1:3F:21:84:EF:C7:FF:E9:37:FB:FE:CD:B6:CA:04:EF:
(0)	45:22:C8:5B:32:02:21:00:F3:94:94:8C:3F:DA:C9:34:
(0)	51:AE:9A:73:07:1B:37:36:DC:28:62:98:D7:5C:66:52:
(0)	98:71:17:EA:46:23:10:97
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AF:67:88:3B:57:B0:4E:DD:8F:A6:D9:7E:F6:2E:A8:EB:
(0)	81:0A:C7:71:60:F0:24:5E:55:D6:0C:2F:E7:85:87:3A
(0)	Timestamp : Oct 22 21:05:01.223 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:D2:A5:92:31:F6:F8:92:C8:0D:45:20:
(0)	A9:43:B4:3D:09:ED:63:29:FE:6C:BF:13:91:72:85:72:
(0)	ED:AF:05:9C:32:02:20:08:8A:F2:6D:EA:45:68:1A:22:
(0)	08:F4:76:CA:54:F5:B5:75:78:5E:A5:3B:2B:94:42:20:
(0)	03:D1:89:A3:78:FC:78
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AC:AB:30:70:6C:EB:EC:84:31:F4:13:D2:F4:91:5F:11:
(0)	1E:42:24:43:B1:F2:A6:8C:4F:3C:2B:3B:A7:1E:02:C3
(0)	Timestamp : Oct 22 21:05:00.999 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:7A:D5:12:14:07:82:C9:A8:23:A7:95:43:
(0)	83:2B:93:B8:98:74:39:EA:8B:81:EE:6B:D9:1C:CB:DB:
(0)	50:74:D2:BA:02:21:00:C0:5F:F6:05:5B:47:AB:76:2E:
(0)	57:C7:FB:81:9B:91:F0:94:D6:15:89:F5:92:BF:31:F6:
(0)	02:CB:61:FB:61:95:9F
(0)Signature	(384 octets)
(0)	6f:c0:09:87:ec:ea:a5:4c:65:e0:96:7f:ee:cd:75:35
(0)	51:57:14:d5:af:5b:ed:55:e5:c4:27:67:93:7e:af:0a
(0)	ad:d2:a5:b9:86:c9:52:60:fc:8e:01:3c:33:bc:68:e2
(0)	7e:29:00:f6:4b:55:d6:1b:1e:a5:3e:e7:65:02:a5:c5
(0)	9d:6a:a2:d2:7e:68:e5:19:af:6d:81:db:29:c8:c8:6b
(0)	20:fa:eb:0b:70:20:be:bc:bb:89:48:ae:d4:d1:a8:ae
(0)	5c:01:be:87:43:5a:c6:43:b6:4a:de:24:a3:02:3b:67
(0)	d4:03:ab:90:d1:68:e0:7f:c7:f5:7d:15:2c:c7:bd:bd
(0)	35:33:ba:a3:1f:c6:a9:57:aa:a6:c7:ad:98:be:2a:8f
(0)	cb:c2:2e:1e:7f:7c:0f:e4:f0:a0:61:5a:24:66:24:ae

(0)	19:1c:8b:9f:3a:bc:a1:b4:47:71:63:43:2c:01:59:7c
(0)	9a:6a:88:aa:5f:f4:91:4a:7f:28:08:7b:61:52:4b:da
(0)	20:a9:e7:0e:35:a9:87:c5:1c:74:86:d2:56:7a:87:eb
(0)	03:73:4c:44:6e:c8:fd:b0:d0:f6:1f:d0:69:82:ab:57
(0)	d4:6d:2c:d7:7b:5a:60:ce:20:2a:6a:1f:0f:43:2a:79
(0)	f0:74:86:d8:6c:dc:86:a5:ca:98:d8:ae:38:79:36:38
(0)	2d:a1:02:36:5d:c2:04:3f:1a:f5:ea:00:99:b7:78:0c
(0)	fe:36:07:9b:5d:21:f9:14:65:37:d8:d8:e5:fd:ee:1a
(0)	c0:c3:a8:d7:0d:d5:a8:d2:0b:da:c5:c8:39:03:52:1d
(0)	84:ec:2d:67:f9:c1:7d:79:56:0b:8d:b4:b8:74:30:63
(0)	4c:02:98:d1:6a:0b:76:e9:72:2d:90:78:ac:96:88:a0
(0)	64:04:46:cd:3f:75:64:2a:79:14:a5:88:48:6d:ed:a2
(0)	e5:8b:eb:10:91:9c:05:2a:32:20:d3:d5:a7:d8:16:1d
(0)	4f:c1:91:ed:6d:93:a3:00:8d:b8:26:d0:cc:47:cf:57
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(1)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(1)Valid From	Mar 22 00:00:00 2021 GMT
(1)Valid Till	Mar 21 23:59:59 2036 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(3072 bit)
(1)	RSA Public-Key: (3072 bit)
(1)	Modulus:
(1)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(1)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(1)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(1)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(1)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(1)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(1)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(1)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(1)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(1)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(1)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(1)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(1)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(1)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(1)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(1)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(1)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(1)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(1)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(1)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(1)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(1)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(1)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:

(1)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(1)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(1)	36:d7:77:f5:91:27:08:66:7b:4d
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(1)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	Policy: 2.23.140.1.2.2
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(1)	OCSP - URI:http://ocsp.sectigo.com
(1)Signature	(512 octets)
(1)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(1)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(1)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(1)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(1)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(1)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(1)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(1)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(1)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(1)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(1)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(1)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(1)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(1)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(1)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(1)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(1)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(1)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(1)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(1)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(1)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(1)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(1)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(1)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(1)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(1)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(1)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(1)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(1)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(1)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(1)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(1)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4

(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(2)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(2)Valid From	Mar 22 00:00:00 2021 GMT
(2)Valid Till	Jan 18 23:59:59 2038 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(2)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(2)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(2)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(2)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(2)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(2)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(2)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(2)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(2)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(2)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(2)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(2)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(2)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(2)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(2)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(2)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(2)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(2)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(2)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(2)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(2)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(2)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(2)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(2)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(2)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(2)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(2)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(2)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(2)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(2)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(2)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(2)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(2)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(2)	7c:6d:cf
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB

(2)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(2)Signature	(512 octets)
(2)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(2)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(2)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(2)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(2)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(2)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(2)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(2)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(2)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(2)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(2)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(2)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(2)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(2)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(2)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(2)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(2)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(2)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(2)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(2)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(2)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(2)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(2)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(2)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(2)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(2)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(2)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(2)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(2)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(2)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(2)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(2)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(3)CERTIFICATE 3	
(3)Version	3 (0x2)
(3)Serial Number	01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d
(3)Signature Algorithm	sha384WithRSAEncryption
(3)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)SUBJECT NAME	

countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)Valid From	Feb 1 00:00:00 2010 GMT
(3)Valid Till	Jan 18 23:59:59 2038 GMT
(3)Public Key Algorithm	rsaEncryption
(3)RSA Public Key	(4096 bit)
(3)	RSA Public-Key: (4096 bit)
(3)	Modulus:
(3)	00:80:12:65:17:36:0e:c3:db:08:b3:d0:ac:57:0d:
(3)	76:ed:cd:27:d3:4c:ad:50:83:61:e2:aa:20:4d:09:
(3)	2d:64:09:dc:ce:89:9f:cc:3d:a9:ec:f6:cf:c1:dc:
(3)	f1:d3:b1:d6:7b:37:28:11:2b:47:da:39:c6:bc:3a:
(3)	19:b4:5f:a6:bd:7d:9d:a3:63:42:b6:76:f2:a9:3b:
(3)	2b:91:f8:e2:6f:d0:ec:16:20:90:09:3e:e2:e8:74:
(3)	c9:18:b4:91:d4:62:64:db:7f:a3:06:f1:88:18:6a:
(3)	90:22:3c:bc:fe:13:f0:87:14:7b:f6:e4:1f:8e:d4:
(3)	e4:51:c6:11:67:46:08:51:cb:86:14:54:3f:bc:33:
(3)	fe:7e:6c:9c:ff:16:9d:18:bd:51:8e:35:a6:a7:66:
(3)	c8:72:67:db:21:66:b1:d4:9b:78:03:c0:50:3a:e8:
(3)	cc:f0:dc:bc:9e:4c:fe:af:05:96:35:1f:57:5a:b7:
(3)	ff:ce:f9:3d:b7:2c:b6:f6:54:dd:c8:e7:12:3a:4d:
(3)	ae:4c:8a:b7:5c:9a:b4:b7:20:3d:ca:7f:22:34:ae:
(3)	7e:3b:68:66:01:44:e7:01:4e:46:53:9b:33:60:f7:
(3)	94:be:53:37:90:73:43:f3:32:c3:53:ef:db:aa:fe:
(3)	74:4e:69:c7:6b:8c:60:93:de:c4:c7:0c:df:e1:32:
(3)	ae:cc:93:3b:51:78:95:67:8b:ee:3d:56:fe:0c:d0:
(3)	69:0f:1b:0f:f3:25:26:6b:33:6d:f7:6e:47:fa:73:
(3)	43:e5:7e:0e:a5:66:b1:29:7c:32:84:63:55:89:c4:
(3)	0d:c1:93:54:30:19:13:ac:d3:7d:37:a7:eb:5d:3a:
(3)	6c:35:5c:db:41:d7:12:da:a9:49:0b:df:d8:80:8a:
(3)	09:93:62:8e:b5:66:cf:25:88:cd:84:b8:b1:3f:a4:
(3)	39:0f:d9:02:9e:eb:12:4c:95:7c:f3:6b:05:a9:5e:
(3)	16:83:cc:b8:67:e2:e8:13:9d:cc:5b:82:d3:4c:b3:
(3)	ed:5b:ff:de:e5:73:ac:23:3b:2d:00:bf:35:55:74:
(3)	09:49:d8:49:58:1a:7f:92:36:e6:51:92:0e:f3:26:
(3)	7d:1c:4d:17:bc:c9:ec:43:26:d0:bf:41:5f:40:a9:
(3)	44:44:f4:99:e7:57:87:9e:50:1f:57:54:a8:3e:fd:
(3)	74:63:2f:b1:50:65:09:e6:58:42:2e:43:1a:4c:b4:
(3)	f0:25:47:59:fa:04:1e:93:d4:26:46:4a:50:81:b2:
(3)	de:be:78:b7:fc:67:15:e1:c9:57:84:1e:0f:63:d6:
(3)	e9:62:ba:d6:5f:55:2e:ea:5c:c6:28:08:04:25:39:
(3)	b8:0e:2b:a9:f2:4c:97:1c:07:3f:0d:52:f5:ed:ef:
(3)	2f:82:0f
(3)	Exponent: 65537 (0x10001)
(3)X509v3 EXTENSIONS	
(3)X509v3 Subject Key Identifier	53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(3)X509v3 Key Usage	critical
(3)	Certificate Sign, CRL Sign
(3)X509v3 Basic Constraints	critical
(3)	CA:TRUE
(3)Signature	(512 octets)
(3)	5c:d4:7c:0d:cf:f7:01:7d:41:99:65:0c:73:c5:52:9f

(3)	cb:f8:cf:99:06:7f:1b:da:43:15:9f:9e:02:55:57:96
(3)	14:f1:52:3c:27:87:94:28:ed:1f:3a:01:37:a2:76:fc
(3)	53:50:c0:84:9b:c6:6b:4e:ba:8c:21:4f:a2:8e:55:62
(3)	91:f3:69:15:d8:bc:88:e3:c4:aa:0b:fd:ef:a8:e9:4b
(3)	55:2a:06:20:6d:55:78:29:19:ee:5f:30:5c:4b:24:11
(3)	55:ff:24:9a:6e:5e:2a:2b:ee:0b:4d:9f:7f:f7:01:38
(3)	94:14:95:43:07:09:fb:60:a9:ee:1c:ab:12:8c:a0:9a
(3)	5e:a7:98:6a:59:6d:8b:3f:08:fb:c8:d1:45:af:18:15
(3)	64:90:12:0f:73:28:2e:c5:e2:24:4e:fc:58:ec:f0:f4
(3)	45:fe:22:b3:eb:2f:8e:d2:d9:45:61:05:c1:97:6f:a8
(3)	76:72:8f:8b:8c:36:af:bf:0d:05:ce:71:8d:e6:a6:6f
(3)	1f:6c:a6:71:62:c5:d8:d0:83:72:0c:f1:67:11:89:0c
(3)	9c:13:4c:72:34:df:bc:d5:71:df:aa:71:dd:e1:b9:6c
(3)	8c:3c:12:5d:65:da:bd:57:12:b6:43:6b:ff:e5:de:4d
(3)	66:11:51:cf:99:ae:ec:17:b6:e8:71:91:8c:de:49:fe
(3)	dd:35:71:a2:15:27:94:1c:cf:61:e3:26:bb:6f:a3:67
(3)	25:21:5d:e6:dd:1d:0b:2e:68:1b:3b:82:af:ec:83:67
(3)	85:d4:98:51:74:b1:b9:99:80:89:ff:7f:78:19:5c:79
(3)	4a:60:2e:92:40:ae:4c:37:2a:2c:c9:c7:62:c8:0e:5d
(3)	f7:36:5b:ca:e0:25:25:01:b4:dd:1a:07:9c:77:00:3f
(3)	d0:dc:d5:ec:3d:d4:fa:bb:3f:cc:85:d6:6f:7f:a9:2d
(3)	df:b9:02:f7:f5:97:9a:b5:35:da:c3:67:b0:87:4a:a9
(3)	28:9e:23:8e:ff:5c:27:6b:e1:b0:4f:f3:07:ee:00:2e
(3)	d4:59:87:cb:52:41:95:ea:f4:47:d7:ee:64:41:55:7c
(3)	8d:59:02:95:dd:62:9d:c2:b9:ee:5a:28:74:84:a5:9b
(3)	b7:90:c7:0c:07:df:f5:89:36:74:32:d6:28:c1:b0:b0
(3)	0b:e0:9c:4c:c3:1c:d6:fc:e3:69:b5:47:46:81:2f:a2
(3)	82:ab:d3:63:44:70:c4:8d:ff:2d:33:ba:ad:8f:7b:b5
(3)	70:88:ae:3e:19:cf:40:28:d8:fc:c8:90:bb:5d:99:22
(3)	f5:52:e6:58:c5:1f:88:31:43:ee:88:1d:d7:c6:8e:3c
(3)	43:6a:1d:a7:18:de:7d:3d:16:f1:62:f9:ca:90:a8:fd
(4)CERTIFICATE 4	
(4)Version	3 (0x2)
(4)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(4)Signature Algorithm	sha384WithRSAEncryption
(4)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(4)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(4)Valid From	Mar 22 00:00:00 2021 GMT
(4)Valid Till	Jan 18 23:59:59 2038 GMT
(4)Public Key Algorithm	rsaEncryption
(4)RSA Public Key	(4096 bit)
(4)	RSA Public-Key: (4096 bit)
(4)	Modulus:
(4)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(4)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(4)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(4)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:

(4)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(4)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(4)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(4)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(4)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(4)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(4)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(4)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(4)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(4)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(4)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(4)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(4)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(4)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(4)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(4)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(4)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(4)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(4)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(4)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(4)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(4)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(4)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(4)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(4)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(4)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(4)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(4)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(4)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(4)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(4)	7c:6d:cf
(4)	Exponent: 65537 (0x10001)
(4)X509v3 EXTENSIONS	
(4)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(4)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(4)X509v3 Key Usage	critical
(4)	Digital Signature, Certificate Sign, CRL Sign
(4)X509v3 Basic Constraints	critical
(4)	CA:TRUE
(4)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(4)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(4)X509v3 CRL Distribution Points	
(4)	Full Name:
(4)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(4)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(4)Signature	(512 octets)
(4)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(4)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(4)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(4)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(4)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(4)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(4)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(4)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(4)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72

(4)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(4)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(4)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(4)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(4)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(4)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(4)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(4)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(4)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(4)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(4)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(4)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(4)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(4)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(4)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(4)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(4)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(4)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(4)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(4)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(4)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(4)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(4)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(5)CERTIFICATE 5	
(5)Version	3 (0x2)
(5)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(5)Signature Algorithm	sha384WithRSAEncryption
(5)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(5)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(5)Valid From	Mar 22 00:00:00 2021 GMT
(5)Valid Till	Mar 21 23:59:59 2036 GMT
(5)Public Key Algorithm	rsaEncryption
(5)RSA Public Key	(3072 bit)
(5)	RSA Public-Key: (3072 bit)
(5)	Modulus:
(5)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(5)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(5)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(5)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(5)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(5)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(5)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(5)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(5)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(5)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(5)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(5)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(5)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(5)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:

(5)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(5)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(5)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(5)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(5)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(5)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(5)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(5)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(5)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(5)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(5)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(5)	36:d7:77:f5:91:27:08:66:7b:4d
(5)	Exponent: 65537 (0x10001)
(5)X509v3 EXTENSIONS	
(5)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(5)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(5)X509v3 Key Usage	critical
(5)	Digital Signature, Certificate Sign, CRL Sign
(5)X509v3 Basic Constraints	critical
(5)	CA:TRUE, pathlen:0
(5)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(5)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(5)	Policy: 2.23.140.1.2.2
(5)X509v3 CRL Distribution Points	
(5)	Full Name:
(5)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(5)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(5)	OCSP - URI:http://ocsp.sectigo.com
(5)Signature	(512 octets)
(5)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(5)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(5)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(5)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(5)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(5)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(5)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(5)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(5)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(5)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(5)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(5)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(5)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(5)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(5)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(5)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(5)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(5)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(5)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(5)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(5)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(5)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(5)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(5)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(5)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(5)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83

(5)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(5)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(5)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(5)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(5)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(5)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c



1 HTTP Response Method and Header Information Collected

port 8093/tcp

QID: 48118
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 07/20/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8093.

GET / HTTP/1.1
 Host: 172.40.123.5:8093
 Connection: Keep-Alive

HTTP/1.1 404 Not Found
 date: Sat, 25 Apr 2026 01:56:17 GMT
 server: unicorn
 content-length: 22
 content-type: application/json



1 Default Web Page

port 9091/tcp over SSL

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:9091
Connection: Keep-Alive

{"detail": "Not Found"}



1 Default Web Page (Follow HTTP Redirection)

port 9091/tcp over SSL

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:9091
Connection: Keep-Alive

{"detail":"Not Found"}



1 SSL Server Information Retrieval

port 9091/tcp over SSL

QID: 38116
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					

SSLv3 PROTOCOL IS DISABLED

TLSv1 PROTOCOL IS DISABLED

TLSv1.1 PROTOCOL IS DISABLED

TLSv1.2 PROTOCOL IS ENABLED

TLSv1.2 COMPRESSION METHOD None

ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1 AES(128)	MEDIUM
----------------------	------	-----	---------------	--------

ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1 AES(256)	HIGH
----------------------	------	-----	---------------	------

TLSv1.3 PROTOCOL IS ENABLED



1 SSL Session Caching Information

port 9091/tcp over SSL

QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 9091/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 9091/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 9091/tcp over SSL

QID: 38706
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no



1 Secure Sockets Layer (SSL) Certificate Transparency Information

port 9091/tcp over SSL

QID: 38718
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.anla.gov.co, O=U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA, ST=Distrito Capital de Bogot, C=CO			
Certificate	no	(unknown)	(unknown)	d809553b944f7affc816196f9 44f85abb0f8fc5e8755260f15 d12e72bb454b14	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	af67883b57b04edd8fa6d97ef 62ea8eb810ac77160f0245e55 d60c2fe785873a	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	acab30706cebec8431f413d2f 4915f111e422443b1f2a68c4f 3c2b3ba71e02c3	Thu 01 Jan 1970 12:00:00 AM GMT



1 Reports if server supports Post Quantum Cryptographic(PQC) Key Exchange Algorithm

port 9091/tcp over SSL

QID: 38994
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

It reports complete list of all host-supported PQC key-exchange algorithms along with full handshake details.
If server hosts any service

over TLS1.3, then a probe is sent to validate if the service supports following PQC key exchange

algorithms.
MLKEM512
MLKEM768
MLKEM1024
X25519MLKEM768
SecP256r1MLKEM768
SecP384r1MLKEM1024

Field

Description

Cipher name
Cipher used

Protocol
TLS

version

Key-exchange
Negotiated PQC KEX

Authentication

Signature algorithm

MAC
Message authentication code

Encryption + key
strength
Encryption mode and key size

NIST security strength
Security strength (NIST
equivalent)

Reference: <https://csrc.nist.gov/groups/ST/post-quantum-crypto/evaluation-criteria.html>

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	STRENGTH
TLS13-AES-256-GCM-SHA384	X25519MLKEM768	RSA-PSS	AEAD	AESGCM(256)	192-bit



1 Reports Signature Algorithm used in Post Quantum Cryptographic(PQC) detection using QID 38994

port 9091/tcp over SSL

QID: 38995
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

If server hosts any service over TLS1.3, then a probe is sent to validate if the service supports PQC key exchange algorithms as part of QID38994.

This QID reports Signature Algorithm used by the service for Post Quantum Cryptographic(PQC) SSL handshake using QID 38994.

It

reports server's preferred PQC signature algorithm.

This QID is planned for future deprecation.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Preferred PQC Signature Algorithm: RSA-PSS



1 TLS Secure Renegotiation Extension Support Information

port 9091/tcp over SSL

QID:	42350
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tier renegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 9091/tcp over SSL

QID: 48340
Category: Information gathering
Associated CVEs: -
Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
Bugtraq ID: -
Service Modified: 04/13/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 9091/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	b2:f8:3d:72:1f:f3:a7:29:60:a2:df:c3:eb:8c:4e:fe
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(0)SUBJECT NAME	
countryName	CO
stateOrProvinceName	Distrito Capital de Bogot\C3\A1
organizationName	U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA
commonName	*.anla.gov.co
(0)Valid From	Oct 22 00:00:00 2025 GMT
(0)Valid Till	Nov 3 23:59:59 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c5:22:80:6e:68:2e:0a:69:6c:67:0c:b8:ee:74:
(0)	e6:56:64:4b:b8:7c:61:47:27:e3:6d:60:a6:34:1e:
(0)	77:20:80:97:2e:ef:ac:2a:8c:52:08:59:9b:33:1e:
(0)	46:70:61:83:8e:1a:85:af:55:76:33:a3:94:c1:04:
(0)	e3:2c:f3:01:07:35:c1:4a:dc:48:47:42:2f:ae:f1:
(0)	fd:b7:49:e5:ff:21:ba:47:cb:bf:1e:4d:13:d3:32:
(0)	17:73:33:65:22:03:ee:2d:36:f2:bc:5a:a5:7d:ad:
(0)	03:01:c2:c0:fe:95:9e:af:81:95:bb:43:59:95:4a:
(0)	bf:82:31:de:e6:1b:43:f4:11:c0:36:be:2c:00:fc:
(0)	2f:97:4b:bb:78:87:61:6e:29:1a:91:8b:a6:2d:f6:
(0)	27:75:93:c2:46:8d:84:cf:b6:8a:69:98:4d:2d:b3:
(0)	4c:1d:44:ea:f6:a4:f9:00:5b:c8:8a:ed:77:66:b3:
(0)	ce:b1:87:b7:e7:52:95:da:e2:08:0d:bb:03:78:02:
(0)	17:46:ce:46:e7:83:f1:1d:ba:47:a3:e2:0e:e3:7b:
(0)	dc:ff:47:79:09:ff:a4:5a:2d:58:4c:d4:1c:24:af:
(0)	a1:aa:ed:50:96:8e:9c:e5:7a:a2:ba:91:53:30:4c:
(0)	42:04:c6:39:7b:c1:f3:88:68:7b:6f:5a:8b:1d:ef:
(0)	5c:5f
(0)	Exponent: 65537 (0x10001)

(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(0)X509v3 Subject Key Identifier	3A:B2:87:43:6F:E2:96:F3:ED:40:44:B2:5F:8C:7E:8B:8F:2C:CD:44
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.1.3.4
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.2
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
(0)	OCSP - URI:http://ocsp.sectigo.com
(0)X509v3 Subject Alternative Name	DNS:*.anla.gov.co, DNS:anla.gov.co
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:
(0)	B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14
(0)	Timestamp : Oct 22 21:05:01.112 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:DB:DF:24:6B:4B:B4:A3:AF:88:F0:38:
(0)	D1:3F:21:84:EF:C7:FF:E9:37:FB:FE:CD:B6:CA:04:EF:
(0)	45:22:C8:5B:32:02:21:00:F3:94:94:8C:3F:DA:C9:34:
(0)	51:AE:9A:73:07:1B:37:36:DC:28:62:98:D7:5C:66:52:
(0)	98:71:17:EA:46:23:10:97
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AF:67:88:3B:57:B0:4E:DD:8F:A6:D9:7E:F6:2E:A8:EB:
(0)	81:0A:C7:71:60:F0:24:5E:55:D6:0C:2F:E7:85:87:3A
(0)	Timestamp : Oct 22 21:05:01.223 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:D2:A5:92:31:F6:F8:92:C8:0D:45:20:
(0)	A9:43:B4:3D:09:ED:63:29:FE:6C:BF:13:91:72:85:72:
(0)	ED:AF:05:9C:32:02:20:08:8A:F2:6D:EA:45:68:1A:22:
(0)	08:F4:76:CA:54:F5:B5:75:78:5E:A5:3B:2B:94:42:20:
(0)	03:D1:89:A3:78:FC:78
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AC:AB:30:70:6C:EB:EC:84:31:F4:13:D2:F4:91:5F:11:
(0)	1E:42:24:43:B1:F2:A6:8C:4F:3C:2B:3B:A7:1E:02:C3
(0)	Timestamp : Oct 22 21:05:00.999 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:7A:D5:12:14:07:82:C9:A8:23:A7:95:43:
(0)	83:2B:93:B8:98:74:39:EA:8B:81:EE:6B:D9:1C:CB:DB:
(0)	50:74:D2:BA:02:21:00:C0:5F:F6:05:5B:47:AB:76:2E:
(0)	57:C7:FB:81:9B:91:F0:94:D6:15:89:F5:92:BF:31:F6:
(0)	02:CB:61:FB:61:95:9F
(0)Signature	(384 octets)
(0)	6f:c0:09:87:ec:ea:a5:4c:65:e0:96:7f:ee:cd:75:35

(0)	51:57:14:d5:af:5b:ed:55:e5:c4:27:67:93:7e:af:0a
(0)	ad:d2:a5:b9:86:c9:52:60:fc:8e:01:3c:33:bc:68:e2
(0)	7e:29:00:f6:4b:55:d6:1b:1e:a5:3e:e7:65:02:a5:c5
(0)	9d:6a:a2:d2:7e:68:e5:19:af:6d:81:db:29:c8:c8:6b
(0)	20:fa:eb:0b:70:20:be:bc:bb:89:48:ae:d4:d1:a8:ae
(0)	5c:01:be:87:43:5a:c6:43:b6:4a:de:24:a3:02:3b:67
(0)	d4:03:ab:90:d1:68:e0:7f:c7:f5:7d:15:2c:c7:bd:bd
(0)	35:33:ba:a3:1f:c6:a9:57:aa:a6:c7:ad:98:be:2a:8f
(0)	cb:c2:2e:1e:7f:7c:0f:e4:f0:a0:61:5a:24:66:24:ae
(0)	19:1c:8b:9f:3a:bc:a1:b4:47:71:63:43:2c:01:59:7c
(0)	9a:6a:88:aa:5f:f4:91:4a:7f:28:08:7b:61:52:4b:da
(0)	20:a9:e7:0e:35:a9:87:c5:1c:74:86:d2:56:7a:87:eb
(0)	03:73:4c:44:6e:c8:fd:b0:d0:f6:1f:d0:69:82:ab:57
(0)	d4:6d:2c:d7:7b:5a:60:ce:20:2a:6a:1f:0f:43:2a:79
(0)	f0:74:86:d8:6c:dc:86:a5:ca:98:d8:ae:38:79:36:38
(0)	2d:a1:02:36:5d:c2:04:3f:1a:f5:ea:00:99:b7:78:0c
(0)	fe:36:07:9b:5d:21:f9:14:65:37:d8:d8:e5:fd:ee:1a
(0)	c0:c3:a8:d7:0d:d5:a8:d2:0b:da:c5:c8:39:03:52:1d
(0)	84:ec:2d:67:f9:c1:7d:79:56:0b:8d:b4:b8:74:30:63
(0)	4c:02:98:d1:6a:0b:76:e9:72:2d:90:78:ac:96:88:a0
(0)	64:04:46:cd:3f:75:64:2a:79:14:a5:88:48:6d:ed:a2
(0)	e5:8b:eb:10:91:9c:05:2a:32:20:d3:d5:a7:d8:16:1d
(0)	4f:c1:91:ed:6d:93:a3:00:8d:b8:26:d0:cc:47:cf:57
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(1)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(1)Valid From	Mar 22 00:00:00 2021 GMT
(1)Valid Till	Mar 21 23:59:59 2036 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(3072 bit)
(1)	RSA Public-Key: (3072 bit)
(1)	Modulus:
(1)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(1)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(1)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(1)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(1)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(1)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(1)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(1)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(1)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(1)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(1)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(1)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(1)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(1)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:

(1)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(1)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(1)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(1)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(1)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(1)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(1)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(1)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(1)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(1)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(1)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(1)	36:d7:77:f5:91:27:08:66:7b:4d
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(1)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	Policy: 2.23.140.1.2.2
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(1)	OCSP - URI:http://ocsp.sectigo.com
(1)Signature	(512 octets)
(1)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(1)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(1)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(1)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(1)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(1)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(1)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(1)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(1)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(1)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(1)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(1)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(1)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(1)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(1)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(1)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(1)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(1)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(1)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(1)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(1)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(1)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(1)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(1)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(1)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(1)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83

(1)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(1)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(1)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(1)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(1)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(1)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(2)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(2)Valid From	Mar 22 00:00:00 2021 GMT
(2)Valid Till	Jan 18 23:59:59 2038 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(2)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(2)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(2)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(2)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(2)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(2)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(2)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(2)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(2)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(2)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(2)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(2)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(2)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(2)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(2)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(2)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(2)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(2)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(2)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(2)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(2)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(2)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(2)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(2)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(2)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(2)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(2)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(2)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:

(2)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(2)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(2)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(2)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(2)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(2)	7c:6d:cf
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(2)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(2)Signature	(512 octets)
(2)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(2)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(2)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(2)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(2)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(2)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(2)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(2)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(2)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(2)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(2)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(2)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(2)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(2)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(2)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(2)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(2)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(2)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(2)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(2)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(2)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(2)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(2)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(2)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(2)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(2)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(2)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(2)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(2)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(2)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(2)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(2)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(3)CERTIFICATE 3	
(3)Version	3 (0x2)

(3)Serial Number	01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d
(3)Signature Algorithm	sha384WithRSAEncryption
(3)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)SUBJECT NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)Valid From	Feb 1 00:00:00 2010 GMT
(3)Valid Till	Jan 18 23:59:59 2038 GMT
(3)Public Key Algorithm	rsaEncryption
(3)RSA Public Key	(4096 bit)
(3)	RSA Public-Key: (4096 bit)
(3)	Modulus:
(3)	00:80:12:65:17:36:0e:c3:db:08:b3:d0:ac:57:0d:
(3)	76:ed:cd:27:d3:4c:ad:50:83:61:e2:aa:20:4d:09:
(3)	2d:64:09:dc:ce:89:9f:cc:3d:a9:ec:f6:cf:c1:dc:
(3)	f1:d3:b1:d6:7b:37:28:11:2b:47:da:39:c6:bc:3a:
(3)	19:b4:5f:a6:bd:7d:9d:a3:63:42:b6:f2:a9:3b:
(3)	2b:91:f8:e2:6f:d0:ec:16:20:90:09:3e:e2:e8:74:
(3)	c9:18:b4:91:d4:62:64:db:7f:a3:06:f1:88:18:6a:
(3)	90:22:3c:bc:fe:13:f0:87:14:7b:f6:e4:1f:8e:d4:
(3)	e4:51:c6:11:67:46:08:51:cb:86:14:54:3f:bc:33:
(3)	fe:7e:6c:9c:ff:16:9d:18:bd:51:8e:35:a6:a7:66:
(3)	c8:72:67:db:21:66:b1:d4:9b:78:03:c0:50:3a:e8:
(3)	cc:f0:dc:bc:9e:4c:fe:af:05:96:35:1f:57:5a:b7:
(3)	ff:ce:f9:3d:b7:2c:b6:f6:54:dd:c8:e7:12:3a:4d:
(3)	ae:4c:8a:b7:5c:9a:b4:b7:20:3d:ca:7f:22:34:ae:
(3)	7e:3b:68:66:01:44:e7:01:4e:46:53:9b:33:60:f7:
(3)	94:be:53:37:90:73:43:f3:32:c3:53:ef:db:aa:fe:
(3)	74:4e:69:c7:6b:8c:60:93:de:c4:c7:0c:df:e1:32:
(3)	ae:cc:93:3b:51:78:95:67:8b:ee:3d:56:fe:0c:d0:
(3)	69:0f:1b:0f:f3:25:26:6b:33:6d:f7:6e:47:fa:73:
(3)	43:e5:7e:0e:a5:66:b1:29:7c:32:84:63:55:89:c4:
(3)	0d:c1:93:54:30:19:13:ac:d3:7d:37:a7:eb:5d:3a:
(3)	6c:35:5c:db:41:d7:12:da:a9:49:0b:df:d8:80:8a:
(3)	09:93:62:8e:b5:66:cf:25:88:cd:84:b8:b1:3f:a4:
(3)	39:0f:d9:02:9e:eb:12:4c:95:7c:f3:6b:05:a9:5e:
(3)	16:83:cc:b8:67:e2:e8:13:9d:cc:5b:82:d3:4c:b3:
(3)	ed:5b:ff:de:e5:73:ac:23:3b:2d:00:bf:35:55:74:
(3)	09:49:d8:49:58:1a:7f:92:36:e6:51:92:0e:f3:26:
(3)	7d:1c:4d:17:bc:c9:ec:43:26:d0:bf:41:5f:40:a9:
(3)	44:44:f4:99:e7:57:87:9e:50:1f:57:54:a8:3e:fd:
(3)	74:63:2f:b1:50:65:09:e6:58:42:2e:43:1a:4c:b4:
(3)	f0:25:47:59:fa:04:1e:93:d4:26:46:4a:50:81:b2:
(3)	de:be:78:b7:fc:67:15:e1:c9:57:84:1e:0f:63:d6:
(3)	e9:62:ba:d6:5f:55:2e:ea:5c:c6:28:08:04:25:39:
(3)	b8:0e:2b:a9:f2:4c:97:1c:07:3f:0d:52:f5:ed:ef:
(3)	2f:82:0f

(3)	Exponent: 65537 (0x10001)
(3)X509v3 EXTENSIONS	
(3)X509v3 Subject Key Identifier	53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(3)X509v3 Key Usage	critical
(3)	Certificate Sign, CRL Sign
(3)X509v3 Basic Constraints	critical
(3)	CA:TRUE
(3)Signature	(512 octets)
(3)	5c:d4:7c:0d:cf:f7:01:7d:41:99:65:0c:73:c5:52:9f
(3)	cb:f8:cf:99:06:7f:1b:da:43:15:9f:9e:02:55:57:96
(3)	14:f1:52:3c:27:87:94:28:ed:1f:3a:01:37:a2:76:fc
(3)	53:50:c0:84:9b:c6:6b:4e:ba:8c:21:4f:a2:8e:55:62
(3)	91:f3:69:15:d8:bc:88:e3:c4:aa:0b:fd:ef:a8:e9:4b
(3)	55:2a:06:20:6d:55:78:29:19:ee:5f:30:5c:4b:24:11
(3)	55:ff:24:9a:6e:5e:2a:2b:ee:0b:4d:9f:7f:f7:01:38
(3)	94:14:95:43:07:09:fb:60:a9:ee:1c:ab:12:8c:a0:9a
(3)	5e:a7:98:6a:59:6d:8b:3f:08:fb:c8:d1:45:af:18:15
(3)	64:90:12:0f:73:28:2e:c5:e2:24:4e:fc:58:ec:f0:f4
(3)	45:fe:22:b3:eb:2f:8e:d2:d9:45:61:05:c1:97:6f:a8
(3)	76:72:8f:8b:8c:36:af:bf:0d:05:ce:71:8d:e6:a6:6f
(3)	1f:6c:a6:71:62:c5:d8:d0:83:72:0c:f1:67:11:89:0c
(3)	9c:13:4c:72:34:df:bc:d5:71:df:aa:71:dd:e1:b9:6c
(3)	8c:3c:12:5d:65:da:bd:57:12:b6:43:6b:ff:e5:de:4d
(3)	66:11:51:cf:99:ae:ec:17:b6:e8:71:91:8c:de:49:fe
(3)	dd:35:71:a2:15:27:94:1c:cf:61:e3:26:bb:6f:a3:67
(3)	25:21:5d:e6:dd:1d:0b:2e:68:1b:3b:82:af:ec:83:67
(3)	85:d4:98:51:74:b1:b9:99:80:89:ff:7f:78:19:5c:79
(3)	4a:60:2e:92:40:ae:4c:37:2a:2c:c9:c7:62:c8:0e:5d
(3)	f7:36:5b:ca:e0:25:25:01:b4:dd:1a:07:9c:77:00:3f
(3)	d0:dc:d5:ec:3d:d4:fa:bb:3f:cc:85:d6:6f:7f:a9:2d
(3)	df:b9:02:f7:f5:97:9a:b5:35:da:c3:67:b0:87:4a:a9
(3)	28:9e:23:8e:ff:5c:27:6b:e1:b0:4f:f3:07:ee:00:2e
(3)	d4:59:87:cb:52:41:95:ea:f4:47:d7:ee:64:41:55:7c
(3)	8d:59:02:95:dd:62:9d:c2:b9:ee:5a:28:74:84:a5:9b
(3)	b7:90:c7:0c:07:df:f5:89:36:74:32:d6:28:c1:b0:b0
(3)	0b:e0:9c:4c:c3:1c:d6:fc:e3:69:b5:47:46:81:2f:a2
(3)	82:ab:d3:63:44:70:c4:8d:ff:2d:33:ba:ad:8f:7b:b5
(3)	70:88:ae:3e:19:cf:40:28:d8:fc:c8:90:bb:5d:99:22
(3)	f5:52:e6:58:c5:1f:88:31:43:ee:88:1d:d7:c6:8e:3c
(3)	43:6a:1d:a7:18:de:7d:3d:16:f1:62:f9:ca:90:a8:fd
(4)CERTIFICATE 4	
(4)Version	3 (0x2)
(4)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(4)Signature Algorithm	sha384WithRSAEncryption
(4)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(4)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(4)Valid From	Mar 22 00:00:00 2021 GMT

(4)Valid Till	Jan 18 23:59:59 2038 GMT
(4)Public Key Algorithm	rsaEncryption
(4)RSA Public Key	(4096 bit)
(4)	RSA Public-Key: (4096 bit)
(4)	Modulus:
(4)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(4)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(4)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(4)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(4)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(4)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(4)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(4)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(4)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(4)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(4)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(4)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(4)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(4)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(4)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(4)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(4)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(4)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(4)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(4)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(4)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(4)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(4)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(4)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(4)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(4)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(4)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(4)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(4)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(4)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(4)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(4)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(4)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(4)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(4)	7c:6d:cf
(4)	Exponent: 65537 (0x10001)
(4)X509v3 EXTENSIONS	
(4)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(4)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(4)X509v3 Key Usage	critical
(4)	Digital Signature, Certificate Sign, CRL Sign
(4)X509v3 Basic Constraints	critical
(4)	CA:TRUE
(4)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(4)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(4)X509v3 CRL Distribution Points	
(4)	Full Name:
(4)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(4)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(4)Signature	(512 octets)

(4)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(4)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(4)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(4)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(4)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(4)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(4)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(4)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(4)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(4)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(4)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(4)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(4)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(4)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(4)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(4)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(4)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(4)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(4)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(4)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(4)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(4)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(4)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(4)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(4)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(4)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(4)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(4)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(4)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(4)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(4)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(4)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(5) CERTIFICATE 5	
(5) Version	3 (0x2)
(5) Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(5) Signature Algorithm	sha384WithRSAEncryption
(5) ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(5) SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(5) Valid From	Mar 22 00:00:00 2021 GMT
(5) Valid Till	Mar 21 23:59:59 2036 GMT
(5) Public Key Algorithm	rsaEncryption
(5) RSA Public Key	(3072 bit)
(5)	RSA Public-Key: (3072 bit)
(5)	Modulus:
(5)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(5)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(5)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(5)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(5)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:

(5)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(5)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(5)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(5)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(5)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(5)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(5)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(5)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(5)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(5)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(5)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(5)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(5)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(5)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(5)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(5)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(5)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(5)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(5)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(5)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(5)	36:d7:77:f5:91:27:08:66:7b:4d
(5)	Exponent: 65537 (0x10001)
(5)X509v3 EXTENSIONS	
(5)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(5)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(5)X509v3 Key Usage	critical
(5)	Digital Signature, Certificate Sign, CRL Sign
(5)X509v3 Basic Constraints	critical
(5)	CA:TRUE, pathlen:0
(5)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(5)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(5)	Policy: 2.23.140.1.2.2
(5)X509v3 CRL Distribution Points	
(5)	Full Name:
(5)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(5)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(5)	OCSP - URI:http://ocsp.sectigo.com
(5)Signature	(512 octets)
(5)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(5)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(5)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(5)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(5)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(5)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(5)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(5)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(5)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(5)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(5)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(5)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(5)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(5)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(5)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(5)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(5)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32

(5)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(5)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(5)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(5)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(5)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(5)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(5)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(5)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(5)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(5)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(5)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(5)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(5)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(5)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(5)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c



1 HTTP Response Method and Header Information Collected

port 9091/tcp

QID: 48118
 Category: Information gathering
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 07/20/2020
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 9091.

GET / HTTP/1.1
 Host: 172.40.123.5:9091

Connection: Keep-Alive

HTTP/1.1 404 Not Found
date: Sat, 25 Apr 2026 02:03:04 GMT
server: uvicorn
content-length: 22
content-type: application/json

1 Default Web Page

port 8088/tcp over SSL

QID: 12230
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8088
Connection: Keep-Alive

{"detail":"Not Found"}

1 Default Web Page (Follow HTTP Redirection)

port 8088/tcp over SSL

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8088
Connection: Keep-Alive

{"detail":"Not Found"}

**1 SSL Server Information Retrieval**

port 8088/tcp over SSL

QID:	38116
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					



1 SSL Session Caching Information

port 8088/tcp over SSL

QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 8088/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 8088/tcp over SSL

QID: 38704
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/01/2023
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						

**1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties**

port 8088/tcp over SSL

QID: 38706
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances

security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no

1 Secure Sockets Layer (SSL) Certificate Transparency Information

port 8088/tcp over SSL

QID: 38718
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.anla.gov.co, O=U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA, ST=Distrito Capital de Bogot, C=CO			
Certificate	no	(unknown)	(unknown)	d809553b944f7affc816196f9 44f85abb0f8fc5e8755260f15 d12e72bb454b14	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	af67883b57b04edd8fa6d97ef 62ea8eb810ac77160f0245e55 d60c2fe785873a	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	acab30706cebec8431f413d2f 4915f111e422443b1f2a68c4f 3c2b3ba71e02c3	Thu 01 Jan 1970 12:00:00 AM GMT



1 Reports if server supports Post Quantum Cryptographic(PQC) Key Exchange Algorithm

port 8088/tcp over SSL

QID: 38994
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

It reports complete list of all host-supported PQC key-exchange algorithms along with full handshake details.
If server hosts any service

over TLS1.3, then a probe is sent to validate if the service supports following PQC key exchange

algorithms.
MLKEM512
MLKEM768
MLKEM1024
X25519MLKEM768
SecP256r1MLKEM768
SecP384r1MLKEM1024

Field

Description

Cipher name
Cipher used

Protocol
TLS

version

Key-exchange
Negotiated PQC KEX

Authentication

Signature algorithm

MAC
Message authentication code

Encryption + key

strength
Encryption mode and key size

NIST security strength
Security strength (NIST

equivalent)

Reference: <https://csrc.nist.gov/groups/ST/post-quantum-crypto/evaluation-criteria.html>

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	STRENGTH
TLS13-AES-256-GCM-SHA384	X25519MLKEM768	RSA-PSS	AEAD	AESGCM(256)	192-bit



1 Reports Signature Algorithm used in Post Quantum Cryptographic(PQC) detection using QID 38994

port 8088/tcp over SSL

QID: 38995
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

If server hosts any service over TLS1.3, then a probe is sent to validate if the service supports PQC key exchange algorithms as part of QID38994. This QID reports Signature Algorithm used by the service for Post Quantum Cryptographic(PQC) SSL handshake using QID 38994.

It reports server's preferred PQC signature algorithm. This QID is planned for future deprecation.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Preferred PQC Signature Algorithm: RSA-PSS

1 TLS Secure Renegotiation Extension Support Information

port 8088/tcp over SSL

QID: 42350
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierrenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 8088/tcp over SSL

QID: 48340
Category: Information gathering
Associated CVEs: -
Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
Bugtraq ID: -
Service Modified: 04/13/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 8088/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -

Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	b2:f8:3d:72:1f:f3:a7:29:60:a2:df:c3:eb:8c:4e:fe
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(0)SUBJECT NAME	
countryName	CO
stateOrProvinceName	Distrito Capital de Bogot\C3A1
organizationName	U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA
commonName	*.anla.gov.co
(0)Valid From	Oct 22 00:00:00 2025 GMT
(0)Valid Till	Nov 3 23:59:59 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c5:22:80:6e:68:2e:0a:69:6c:67:0c:b8:ee:74:
(0)	e6:56:64:4b:b8:7c:61:47:27:e3:6d:60:a6:34:1e:
(0)	77:20:80:97:2e:ef:ac:2a:8c:52:08:59:9b:33:1e:
(0)	46:70:61:83:8e:1a:85:af:55:76:33:a3:94:c1:04:
(0)	e3:2c:f3:01:07:35:c1:4a:dc:48:47:42:2f:ae:f1:
(0)	fd:b7:49:e5:ff:21:ba:47:cb:bf:1e:4d:13:d3:32:
(0)	17:73:33:65:22:03:ee:2d:36:f2:bc:5a:a5:7d:ad:
(0)	03:01:c2:c0:fe:95:9e:af:81:95:bb:43:59:95:4a:
(0)	bf:82:31:de:e6:1b:43:f4:11:c0:36:be:2c:00:fc:

(0)	2f:97:4b:bb:78:87:61:6e:29:1a:91:8b:a6:2d:f6:
(0)	27:75:93:c2:46:8d:84:cf:b6:8a:69:98:4d:2d:b3:
(0)	4c:1d:44:ea:f6:a4:f9:00:5b:c8:8a:ed:77:66:b3:
(0)	ce:b1:87:b7:e7:52:95:da:e2:08:0d:bb:03:78:02:
(0)	17:46:ce:46:e7:83:f1:1d:ba:47:a3:e2:0e:e3:7b:
(0)	dc:ff:47:79:09:ff:a4:5a:2d:58:4c:d4:1c:24:af:
(0)	a1:aa:ed:50:96:8e:9c:e5:7a:a2:ba:91:53:30:4c:
(0)	42:04:c6:39:7b:c1:f3:88:68:7b:6f:5a:8b:1d:ef:
(0)	5c:5f
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(0)X509v3 Subject Key Identifier	3A:B2:87:43:6F:E2:96:F3:ED:40:44:B2:5F:8C:7E:8B:8F:2C:CD:44
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.1.3.4
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.2
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
(0)	OCSP - URI:http://ocsp.sectigo.com
(0)X509v3 Subject Alternative Name	DNS:*.anla.gov.co, DNS:anla.gov.co
(0)CT Precertificate SCTs	
Signed Certificate Timestamp:	
(0)	Version : v1 (0x0)
(0)	Log ID : D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:
(0)	B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14
(0)	Timestamp : Oct 22 21:05:01.112 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:DB:DF:24:6B:4B:B4:A3:AF:88:F0:38:
(0)	D1:3F:21:84:EF:C7:FF:E9:37:FB:FE:CD:B6:CA:04:EF:
(0)	45:22:C8:5B:32:02:21:00:F3:94:94:8C:3F:DA:C9:34:
(0)	51:AE:9A:73:07:1B:37:36:DC:28:62:98:D7:5C:66:52:
(0)	98:71:17:EA:46:23:10:97
Signed Certificate Timestamp:	
(0)	Version : v1 (0x0)
(0)	Log ID : AF:67:88:3B:57:B0:4E:DD:8F:A6:D9:7E:F6:2E:A8:EB:
(0)	81:0A:C7:71:60:F0:24:5E:55:D6:0C:2F:E7:85:87:3A
(0)	Timestamp : Oct 22 21:05:01.223 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:D2:A5:92:31:F6:F8:92:C8:0D:45:20:
(0)	A9:43:B4:3D:09:ED:63:29:FE:6C:BF:13:91:72:85:72:
(0)	ED:AF:05:9C:32:02:20:08:8A:F2:6D:EA:45:68:1A:22:
(0)	08:F4:76:CA:54:F5:B5:75:78:5E:A5:3B:2B:94:42:20:
(0)	03:D1:89:A3:78:FC:78
Signed Certificate Timestamp:	
(0)	Version : v1 (0x0)
(0)	Log ID : AC:AB:30:70:6C:EB:EC:84:31:F4:13:D2:F4:91:5F:11:
(0)	1E:42:24:43:B1:F2:A6:8C:4F:3C:2B:3B:A7:1E:02:C3

(0)	Timestamp : Oct 22 21:05:00.999 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:7A:D5:12:14:07:82:C9:A8:23:A7:95:43:
(0)	83:2B:93:B8:98:74:39:EA:8B:81:EE:6B:D9:1C:CB:DB:
(0)	50:74:D2:BA:02:21:00:C0:5F:F6:05:5B:47:AB:76:2E:
(0)	57:C7:FB:81:9B:91:F0:94:D6:15:89:F5:92:BF:31:F6:
(0)	02:CB:61:FB:61:95:9F
(0)Signature	(384 octets)
(0)	6f:c0:09:87:ec:ea:a5:4c:65:e0:96:7f:ee:cd:75:35
(0)	51:57:14:d5:af:5b:ed:55:e5:c4:27:67:93:7e:af:0a
(0)	ad:d2:a5:b9:86:c9:52:60:fc:8e:01:3c:33:bc:68:e2
(0)	7e:29:00:f6:4b:55:d6:1b:1e:a5:3e:e7:65:02:a5:c5
(0)	9d:6a:a2:d2:7e:68:e5:19:af:6d:81:db:29:c8:c8:6b
(0)	20:fa:eb:0b:70:20:be:bc:bb:89:48:ae:d4:d1:a8:ae
(0)	5c:01:be:87:43:5a:c6:43:b6:4a:de:24:a3:02:3b:67
(0)	d4:03:ab:90:d1:68:e0:7f:c7:f5:7d:15:2c:c7:bd:bd
(0)	35:33:ba:a3:1f:c6:a9:57:aa:a6:c7:ad:98:be:2a:8f
(0)	cb:c2:2e:1e:7f:7c:0f:e4:f0:a0:61:5a:24:66:24:ae
(0)	19:1c:8b:9f:3a:bc:a1:b4:47:71:63:43:2c:01:59:7c
(0)	9a:6a:88:aa:5f:f4:91:4a:7f:28:08:7b:61:52:4b:da
(0)	20:a9:e7:0e:35:a9:87:c5:1c:74:86:d2:56:7a:87:eb
(0)	03:73:4c:44:6e:c8:fd:b0:d0:f6:1f:d0:69:82:ab:57
(0)	d4:6d:2c:d7:7b:5a:60:ce:20:2a:6a:1f:0f:43:2a:79
(0)	f0:74:86:d8:6c:dc:86:a5:ca:98:d8:ae:38:79:36:38
(0)	2d:a1:02:36:5d:c2:04:3f:1a:f5:ea:00:99:b7:78:0c
(0)	fe:36:07:9b:5d:21:f9:14:65:37:d8:d8:e5:fd:ee:1a
(0)	c0:c3:a8:d7:0d:d5:a8:d2:0b:da:c5:c8:39:03:52:1d
(0)	84:ec:2d:67:f9:c1:7d:79:56:0b:8d:b4:b8:74:30:63
(0)	4c:02:98:d1:6a:0b:76:e9:72:2d:90:78:ac:96:88:a0
(0)	64:04:46:cd:3f:75:64:2a:79:14:a5:88:48:6d:ed:a2
(0)	e5:8b:eb:10:91:9c:05:2a:32:20:d3:d5:a7:d8:16:1d
(0)	4f:c1:91:ed:6d:93:a3:00:8d:b8:26:d0:cc:47:cf:57
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(1)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(1)Valid From	Mar 22 00:00:00 2021 GMT
(1)Valid Till	Mar 21 23:59:59 2036 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(3072 bit)
(1)	RSA Public-Key: (3072 bit)
(1)	Modulus:
(1)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(1)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(1)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(1)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:

(1)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(1)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(1)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(1)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(1)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(1)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(1)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(1)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(1)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(1)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(1)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(1)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(1)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(1)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(1)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(1)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(1)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(1)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(1)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(1)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(1)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(1)	36:d7:77:f5:91:27:08:66:7b:4d
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(1)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	Policy: 2.23.140.1.2.2
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(1)	OCSP - URI:http://ocsp.sectigo.com
(1)Signature	(512 octets)
(1)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(1)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(1)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(1)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(1)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(1)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(1)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(1)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(1)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(1)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(1)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(1)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(1)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(1)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(1)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(1)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db

(1)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(1)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(1)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(1)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(1)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(1)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(1)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(1)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(1)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(1)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(1)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(1)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(1)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(1)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(1)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(1)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(2)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(2)Valid From	Mar 22 00:00:00 2021 GMT
(2)Valid Till	Jan 18 23:59:59 2038 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(2)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(2)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(2)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(2)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(2)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(2)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(2)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(2)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(2)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(2)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(2)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(2)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(2)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(2)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(2)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(2)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(2)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(2)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:

(2)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(2)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(2)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(2)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(2)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(2)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(2)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(2)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(2)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(2)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(2)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(2)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(2)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(2)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(2)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(2)	7c:6d:cf
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(2)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(2)Signature	(512 octets)
(2)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(2)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(2)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(2)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(2)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(2)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(2)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(2)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(2)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(2)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(2)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(2)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(2)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(2)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(2)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(2)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(2)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(2)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(2)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(2)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(2)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(2)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(2)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(2)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4

(2)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(2)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(2)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(2)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(2)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(2)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(2)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(2)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(3)CERTIFICATE 3	
(3)Version	3 (0x2)
(3)Serial Number	01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d
(3)Signature Algorithm	sha384WithRSAEncryption
(3)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)SUBJECT NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)Valid From	Feb 1 00:00:00 2010 GMT
(3)Valid Till	Jan 18 23:59:59 2038 GMT
(3)Public Key Algorithm	rsaEncryption
(3)RSA Public Key	(4096 bit)
(3)	RSA Public-Key: (4096 bit)
(3)	Modulus:
(3)	00:80:12:65:17:36:0e:c3:db:08:b3:d0:ac:57:0d:
(3)	76:ed:cd:27:d3:4c:ad:50:83:61:e2:aa:20:4d:09:
(3)	2d:64:09:dc:ce:89:9f:cc:3d:a9:ec:f6:cf:c1:dc:
(3)	f1:d3:b1:d6:7b:37:28:11:2b:47:da:39:c6:bc:3a:
(3)	19:b4:5f:a6:bd:7d:9d:a3:63:42:b6:76:f2:a9:3b:
(3)	2b:91:f8:e2:6f:d0:ec:16:20:90:09:3e:e2:e8:74:
(3)	c9:18:b4:91:d4:62:64:db:7f:a3:06:f1:88:18:6a:
(3)	90:22:3c:bc:fe:13:f0:87:14:7b:f6:e4:1f:8e:d4:
(3)	e4:51:c6:11:67:46:08:51:cb:86:14:54:3f:bc:33:
(3)	fe:7e:6c:9c:ff:16:9d:18:bd:51:8e:35:a6:a7:66:
(3)	c8:72:67:db:21:66:b1:d4:9b:78:03:c0:50:3a:e8:
(3)	cc:f0:dc:bc:9e:4c:fe:af:05:96:35:1f:57:5a:b7:
(3)	ff:ce:f9:3d:b7:2c:b6:f6:54:dd:c8:e7:12:3a:4d:
(3)	ae:4c:8a:b7:5c:9a:b4:b7:20:3d:ca:7f:22:34:ae:
(3)	7e:3b:68:66:01:44:e7:01:4e:46:53:9b:33:60:f7:
(3)	94:be:53:37:90:73:43:f3:32:c3:53:ef:db:aa:fe:
(3)	74:4e:69:c7:6b:8c:60:93:de:c4:c7:0c:df:e1:32:
(3)	ae:cc:93:3b:51:78:95:67:8b:ee:3d:56:fe:0c:d0:
(3)	69:0f:1b:0f:f3:25:26:6b:33:6d:f7:6e:47:fa:73:
(3)	43:e5:7e:0e:a5:66:b1:29:7c:32:84:63:55:89:c4:
(3)	0d:c1:93:54:30:19:13:ac:d3:7d:37:a7:eb:5d:3a:
(3)	6c:35:5c:db:41:d7:12:da:a9:49:0b:df:d8:80:8a:
(3)	09:93:62:8e:b5:66:cf:25:88:cd:84:b8:b1:3f:a4:
(3)	39:0f:d9:02:9e:eb:12:4c:95:7c:f3:6b:05:a9:5e:
(3)	16:83:cc:b8:67:e2:e8:13:9d:cc:5b:82:d3:4c:b3:

(3)	ed:5b:ff:de:e5:73:ac:23:3b:2d:00:bf:35:55:74:
(3)	09:49:d8:49:58:1a:7f:92:36:e6:51:92:0e:f3:26:
(3)	7d:1c:4d:17:bc:c9:ec:43:26:d0:bf:41:5f:40:a9:
(3)	44:44:f4:99:e7:57:87:9e:50:1f:57:54:a8:3e:fd:
(3)	74:63:2f:b1:50:65:09:e6:58:42:2e:43:1a:4c:b4:
(3)	f0:25:47:59:fa:04:1e:93:d4:26:46:4a:50:81:b2:
(3)	de:be:78:b7:fc:67:15:e1:c9:57:84:1e:0f:63:d6:
(3)	e9:62:ba:d6:5f:55:2e:ea:5c:c6:28:08:04:25:39:
(3)	b8:0e:2b:a9:f2:4c:97:1c:07:3f:0d:52:f5:ed:ef:
(3)	2f:82:0f
(3)	Exponent: 65537 (0x10001)
(3)X509v3 EXTENSIONS	
(3)X509v3 Subject Key Identifier	53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(3)X509v3 Key Usage	critical
(3)	Certificate Sign, CRL Sign
(3)X509v3 Basic Constraints	critical
(3)	CA:TRUE
(3)Signature	(512 octets)
(3)	5c:d4:7c:0d:cf:f7:01:7d:41:99:65:0c:73:c5:52:9f
(3)	cb:f8:cf:99:06:7f:1b:da:43:15:9f:9e:02:55:57:96
(3)	14:f1:52:3c:27:87:94:28:ed:1f:3a:01:37:a2:76:fc
(3)	53:50:c0:84:9b:c6:6b:4e:ba:8c:21:4f:a2:8e:55:62
(3)	91:f3:69:15:d8:bc:88:e3:c4:aa:0b:fd:ef:a8:e9:4b
(3)	55:2a:06:20:6d:55:78:29:19:ee:5f:30:5c:4b:24:11
(3)	55:ff:24:9a:6e:5e:2a:2b:ee:0b:4d:9f:7f:f7:01:38
(3)	94:14:95:43:07:09:fb:60:a9:ee:1c:ab:12:8c:a0:9a
(3)	5e:a7:98:6a:59:6d:8b:3f:08:fb:c8:d1:45:af:18:15
(3)	64:90:12:0f:73:28:2e:c5:e2:24:4e:fc:58:ec:f0:f4
(3)	45:fe:22:b3:eb:2f:8e:d2:d9:45:61:05:c1:97:6f:a8
(3)	76:72:8f:8b:8c:36:af:bf:0d:05:ce:71:8d:e6:a6:6f
(3)	1f:6c:a6:71:62:c5:d8:d0:83:72:0c:f1:67:11:89:0c
(3)	9c:13:4c:72:34:df:bc:d5:71:df:aa:71:dd:e1:b9:6c
(3)	8c:3c:12:5d:65:da:bd:57:12:b6:43:6b:ff:e5:de:4d
(3)	66:11:51:cf:99:ae:ec:17:b6:e8:71:91:8c:de:49:fe
(3)	dd:35:71:a2:15:27:94:1c:cf:61:e3:26:bb:6f:a3:67
(3)	25:21:5d:e6:dd:1d:0b:2e:68:1b:3b:82:af:ec:83:67
(3)	85:d4:98:51:74:b1:b9:99:80:89:ff:7f:78:19:5c:79
(3)	4a:60:2e:92:40:ae:4c:37:2a:2c:c9:c7:62:c8:0e:5d
(3)	f7:36:5b:ca:e0:25:25:01:b4:dd:1a:07:9c:77:00:3f
(3)	d0:dc:d5:ec:3d:d4:fa:bb:3f:cc:85:d6:6f:7f:a9:2d
(3)	df:b9:02:f7:f5:97:9a:b5:35:da:c3:67:b0:87:4a:a9
(3)	28:9e:23:8e:ff:5c:27:6b:e1:b0:4f:f3:07:ee:00:2e
(3)	d4:59:87:cb:52:41:95:ea:f4:47:d7:ee:64:41:55:7c
(3)	8d:59:02:95:dd:62:9d:c2:b9:ee:5a:28:74:84:a5:9b
(3)	b7:90:c7:0c:07:df:f5:89:36:74:32:d6:28:c1:b0:b0
(3)	0b:e0:9c:4c:c3:1c:d6:fc:e3:69:b5:47:46:81:2f:a2
(3)	82:ab:d3:63:44:70:c4:8d:ff:2d:33:ba:ad:8f:7b:b5
(3)	70:88:ae:3e:19:cf:40:28:d8:fc:c8:90:bb:5d:99:22
(3)	f5:52:e6:58:c5:1f:88:31:43:ee:88:1d:d7:c6:8e:3c
(3)	43:6a:1d:a7:18:de:7d:3d:16:f1:62:f9:ca:90:a8:fd
(4)CERTIFICATE 4	
(4)Version	3 (0x2)
(4)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(4)Signature Algorithm	sha384WithRSAEncryption
(4)ISSUER NAME	

countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(4)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(4)Valid From	Mar 22 00:00:00 2021 GMT
(4)Valid Till	Jan 18 23:59:59 2038 GMT
(4)Public Key Algorithm	rsaEncryption
(4)RSA Public Key	(4096 bit)
(4)	RSA Public-Key: (4096 bit)
(4)	Modulus:
(4)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(4)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(4)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(4)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(4)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(4)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(4)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(4)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(4)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(4)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(4)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(4)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(4)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(4)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(4)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(4)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(4)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(4)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(4)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(4)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(4)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(4)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(4)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(4)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(4)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(4)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(4)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(4)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(4)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(4)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(4)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(4)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(4)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(4)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(4)	7c:6d:cf
(4)	Exponent: 65537 (0x10001)
(4)X509v3 EXTENSIONS	
(4)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(4)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(4)X509v3 Key Usage	critical

(4)	Digital Signature, Certificate Sign, CRL Sign
(4)X509v3 Basic Constraints	critical
(4)	CA:TRUE
(4)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(4)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(4)X509v3 CRL Distribution Points	
(4)	Full Name:
(4)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(4)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(4)Signature	(512 octets)
(4)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(4)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(4)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(4)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(4)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(4)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(4)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(4)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(4)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(4)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(4)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(4)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(4)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(4)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(4)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(4)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(4)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(4)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(4)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(4)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(4)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(4)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(4)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(4)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(4)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(4)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(4)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(4)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(4)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(4)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(4)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(4)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(5)CERTIFICATE 5	
(5)Version	3 (0x2)
(5)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(5)Signature Algorithm	sha384WithRSAEncryption
(5)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(5)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(5)Valid From	Mar 22 00:00:00 2021 GMT

(5)Valid Till	Mar 21 23:59:59 2036 GMT
(5)Public Key Algorithm	rsaEncryption
(5)RSA Public Key	(3072 bit)
(5)	RSA Public-Key: (3072 bit)
(5)	Modulus:
(5)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(5)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(5)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(5)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(5)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(5)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(5)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(5)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(5)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(5)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(5)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(5)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(5)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(5)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(5)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(5)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(5)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(5)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(5)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(5)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(5)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(5)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(5)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(5)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(5)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(5)	36:d7:77:f5:91:27:08:66:7b:4d
(5)	Exponent: 65537 (0x10001)
(5)X509v3 EXTENSIONS	
(5)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(5)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(5)X509v3 Key Usage	critical
(5)	Digital Signature, Certificate Sign, CRL Sign
(5)X509v3 Basic Constraints	critical
(5)	CA:TRUE, pathlen:0
(5)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(5)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(5)	Policy: 2.23.140.1.2.2
(5)X509v3 CRL Distribution Points	
(5)	Full Name:
(5)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(5)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(5)	OCSP - URI:http://ocsp.sectigo.com
(5)Signature	(512 octets)
(5)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(5)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(5)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(5)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(5)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(5)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(5)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40

(5)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(5)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(5)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(5)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(5)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(5)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(5)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(5)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(5)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(5)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(5)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(5)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(5)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(5)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(5)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(5)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(5)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(5)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(5)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(5)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(5)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(5)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(5)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(5)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(5)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c



1 Default Web Page

port 8091/tcp over SSL

QID: 12230
 Category: CGI
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 03/15/2019
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8091
Connection: Keep-Alive

```
{"name":"Eureka ANLA (API)","version":"1.0.0"}
```

1 Default Web Page (Follow HTTP Redirection)

port 8091/tcp over SSL

QID: 13910
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/05/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host: 172.40.123.5:8091
Connection: Keep-Alive

```
{"name":"Eureka ANLA (API)","version":"1.0.0"}
```

1 SSL Server Information Retrieval

port 8091/tcp over SSL

QID: 38116
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No

PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					



1 SSL Session Caching Information

port 8091/tcp over SSL

QID: 38291
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to

establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 8091/tcp over SSL

QID: 38597
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

**1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods**

port 8091/tcp over SSL

QID: 38704
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 02/01/2023
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2						
ECDHE-RSA-AES256-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES256-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES256-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES256-SHA	ECDHE	secp521r1	521	yes	260	low
ECDHE-RSA-AES128-SHA	ECDHE	x25519	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	secp256r1	256	yes	128	low
ECDHE-RSA-AES128-SHA	ECDHE	x448	448	yes	224	low
ECDHE-RSA-AES128-SHA	ECDHE	secp384r1	384	yes	192	low
ECDHE-RSA-AES128-SHA	ECDHE	secp521r1	521	yes	260	low
TLSv1.3						



QID: 38706
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/08/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.3	
Heartbeat	no
OCSP stapling	no
SCT extension	no

QID: 38718
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 06/08/2021
 User Modified: -
 Edited: No
 PCI Vuln: No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.anla.gov.co, O=U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA, ST=Distrito Capital de Bogot, C=CO			
Certificate	no	(unknown)	(unknown)	d809553b944f7affc816196f9 44f85abb0f8fc5e8755260f15 d12e72bb454b14	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	af67883b57b04edd8fa6d97ef 62ea8eb810ac77160f0245e55 d60c2fe785873a	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	acab30706cebec8431f413d2f 4915f111e422443b1f2a68c4f 3c2b3ba71e02c3	Thu 01 Jan 1970 12:00:00 AM GMT

QID: 38994
 Category: General remote services
 Associated CVEs: -
 Vendor Reference: -
 Bugtraq ID: -
 Service Modified: 01/05/2026

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

It reports complete list of all host-supported PQC key-exchange algorithms along with full handshake details.
If server hosts any service

over TLS1.3, then a probe is sent to validate if the service supports following PQC key exchange

algorithms.
MLKEM512
MLKEM768
MLKEM1024
X25519MLKEM768
SecP256r1MLKEM768
SecP384r1MLKEM1024

Field
Description
Cipher name
Cipher used
Protocol
TLS
version
Key-exchange
Negotiated PQC KEX
Authentication
Signature algorithm
MAC
Message authentication code
Encryption + key
strength
Encryption mode and key size
NIST security strength
Security strength (NIST
equivalent)

Reference: <https://csrc.nist.gov/groups/ST/post-quantum-crypto/evaluation-criteria.html>

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	STRENGTH
TLS13-AES-256-GCM-SHA384	X25519MLKEM768	RSA-PSS	AEAD	AESGCM(256)	192-bit



1 Reports Signature Algorithm used in Post Quantum Cryptographic(PQC) detection using QID 38994

port 8091/tcp over SSL

QID: 38995
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/05/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

If server hosts any service over TLS1.3, then a probe is sent to validate if the service supports PQC key exchange algorithms as part of QID38994.
This QID reports Signature Algorithm used by the service for Post Quantum Cryptographic(PQC) SSL handshake using QID 38994.

It
reports server's preferred PQC signature algorithm.
This QID is planned for future deprecation.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Preferred PQC Signature Algorithm: RSA-PSS



1 TLS Secure Renegotiation Extension Support Information

port 8091/tcp over SSL

QID: 42350
Category: General remote services
Associated CVEs: -

Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tier negotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.



1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.2)

port 8091/tcp over SSL

QID: 48340
Category: Information gathering
Associated CVEs: -
Vendor Reference: [SSL/TLS Server supports TLSv1.2](#)
Bugtraq ID: -
Service Modified: 04/13/2026
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

N/A

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 is supported



1 SSL Certificate - Information

port 8091/tcp over SSL

QID: 86002
Category: Web server
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/07/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	b2:f8:3d:72:1f:f3:a7:29:60:a2:df:c3:eb:8c:4e:fe
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(0)SUBJECT NAME	

countryName	CO
stateOrProvinceName	Distrito Capital de Bogot\C3VA1
organizationName	U A E AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA
commonName	*.anla.gov.co
(0)Valid From	Oct 22 00:00:00 2025 GMT
(0)Valid Till	Nov 3 23:59:59 2026 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c5:22:80:6e:68:2e:0a:69:6c:67:0c:b8:ee:74:
(0)	e6:56:64:4b:b8:7c:61:47:27:e3:6d:60:a6:34:1e:
(0)	77:20:80:97:2e:ef:ac:2a:8c:52:08:59:9b:33:1e:
(0)	46:70:61:83:8e:1a:85:af:55:76:33:a3:94:c1:04:
(0)	e3:2c:f3:01:07:35:c1:4a:dc:48:47:42:2f:ae:f1:
(0)	fd:b7:49:e5:ff:21:ba:47:cb:bf:1e:4d:13:d3:32:
(0)	17:73:33:65:22:03:ee:2d:36:f2:bc:5a:a5:7d:ad:
(0)	03:01:c2:c0:fe:95:9e:af:81:95:bb:43:59:95:4a:
(0)	bf:82:31:de:e6:1b:43:f4:11:c0:36:be:2c:00:fc:
(0)	2f:97:4b:bb:78:87:61:6e:29:1a:91:8b:a6:2d:f6:
(0)	27:75:93:c2:46:8d:84:cf:b6:8a:69:98:4d:2d:b3:
(0)	4c:1d:44:ea:f6:a4:f9:00:5b:c8:8a:ed:77:66:b3:
(0)	ce:b1:87:b7:e7:52:95:da:e2:08:0d:bb:03:78:02:
(0)	17:46:ce:46:e7:83:f1:1d:ba:47:a3:e2:0e:e3:7b:
(0)	dc:ff:47:79:09:ff:a4:5a:2d:58:4c:d4:1c:24:af:
(0)	a1:aa:ed:50:96:8e:9c:e5:7a:a2:ba:91:53:30:4c:
(0)	42:04:c6:39:7b:c1:f3:88:68:7b:6f:5a:8b:1d:ef:
(0)	5c:5f
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(0)X509v3 Subject Key Identifier	3A:B2:87:43:6F:E2:96:F3:ED:40:44:B2:5F:8C:7E:8B:8F:2C:CD:44
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.1.3.4
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.2
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI: http://crl.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crl
(0)Authority Information Access	CA Issuers - URI: http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
(0)	OCSP - URI: http://ocsp.sectigo.com
(0)X509v3 Subject Alternative Name	DNS:*.anla.gov.co, DNS:anla.gov.co
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:
(0)	B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14
(0)	Timestamp : Oct 22 21:05:01.112 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:DB:DF:24:6B:4B:B4:A3:AF:88:F0:38:
(0)	D1:3F:21:84:EF:C7:FF:E9:37:FB:FE:CD:B6:CA:04:EF:

(0)	45:22:C8:5B:32:02:21:00:F3:94:94:8C:3F:DA:C9:34:
(0)	51:AE:9A:73:07:1B:37:36:DC:28:62:98:D7:5C:66:52:
(0)	98:71:17:EA:46:23:10:97
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AF:67:88:3B:57:B0:4E:DD:8F:A6:D9:7E:F6:2E:A8:EB:
(0)	81:0A:C7:71:60:F0:24:5E:55:D6:0C:2F:E7:85:87:3A
(0)	Timestamp : Oct 22 21:05:01.223 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:D2:A5:92:31:F6:F8:92:C8:0D:45:20:
(0)	A9:43:B4:3D:09:ED:63:29:FE:6C:BF:13:91:72:85:72:
(0)	ED:AF:05:9C:32:02:20:08:8A:F2:6D:EA:45:68:1A:22:
(0)	08:F4:76:CA:54:F5:B5:75:78:5E:A5:3B:2B:94:42:20:
(0)	03:D1:89:A3:78:FC:78
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : AC:AB:30:70:6C:EB:EC:84:31:F4:13:D2:F4:91:5F:11:
(0)	1E:42:24:43:B1:F2:A6:8C:4F:3C:2B:3B:A7:1E:02:C3
(0)	Timestamp : Oct 22 21:05:00.999 2025 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:7A:D5:12:14:07:82:C9:A8:23:A7:95:43:
(0)	83:2B:93:B8:98:74:39:EA:8B:81:EE:6B:D9:1C:CB:DB:
(0)	50:74:D2:BA:02:21:00:C0:5F:F6:05:5B:47:AB:76:2E:
(0)	57:C7:FB:81:9B:91:F0:94:D6:15:89:F5:92:BF:31:F6:
(0)	02:CB:61:FB:61:95:9F
(0)Signature	(384 octets)
(0)	6f:c0:09:87:ec:ea:a5:4c:65:e0:96:7f:ee:cd:75:35
(0)	51:57:14:d5:af:5b:ed:55:e5:c4:27:67:93:7e:af:0a
(0)	ad:d2:a5:b9:86:c9:52:60:fc:8e:01:3c:33:bc:68:e2
(0)	7e:29:00:f6:4b:55:d6:1b:1e:a5:3e:e7:65:02:a5:c5
(0)	9d:6a:a2:d2:7e:68:e5:19:af:6d:81:db:29:c8:c8:6b
(0)	20:fa:eb:0b:70:20:be:bc:bb:89:48:ae:d4:d1:a8:ae
(0)	5c:01:be:87:43:5a:c6:43:b6:4a:de:24:a3:02:3b:67
(0)	d4:03:ab:90:d1:68:e0:7f:c7:f5:7d:15:2c:c7:bd:bd
(0)	35:33:ba:a3:1f:c6:a9:57:aa:a6:c7:ad:98:be:2a:8f
(0)	cb:c2:2e:1e:7f:7c:0f:e4:f0:a0:61:5a:24:66:24:ae
(0)	19:1c:8b:9f:3a:bc:a1:b4:47:71:63:43:2c:01:59:7c
(0)	9a:6a:88:aa:5f:f4:91:4a:7f:28:08:7b:61:52:4b:da
(0)	20:a9:e7:0e:35:a9:87:c5:1c:74:86:d2:56:7a:87:eb
(0)	03:73:4c:44:6e:c8:fd:b0:d0:f6:1f:d0:69:82:ab:57
(0)	d4:6d:2c:d7:7b:5a:60:ce:20:2a:6a:1f:0f:43:2a:79
(0)	f0:74:86:d8:6c:dc:86:a5:ca:98:d8:ae:38:79:36:38
(0)	2d:a1:02:36:5d:c2:04:3f:1a:f5:ea:00:99:b7:78:0c
(0)	fe:36:07:9b:5d:21:f9:14:65:37:d8:d8:e5:fd:ee:1a
(0)	c0:c3:a8:d7:0d:d5:a8:d2:0b:da:c5:c8:39:03:52:1d
(0)	84:ec:2d:67:f9:c1:7d:79:56:0b:8d:b4:b8:74:30:63
(0)	4c:02:98:d1:6a:0b:76:e9:72:2d:90:78:ac:96:88:a0
(0)	64:04:46:cd:3f:75:64:2a:79:14:a5:88:48:6d:ed:a2
(0)	e5:8b:eb:10:91:9c:05:2a:32:20:d3:d5:a7:d8:16:1d
(0)	4f:c1:91:ed:6d:93:a3:00:8d:b8:26:d0:cc:47:cf:57
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71

(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(1)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(1)Valid From	Mar 22 00:00:00 2021 GMT
(1)Valid Till	Mar 21 23:59:59 2036 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(3072 bit)
(1)	RSA Public-Key: (3072 bit)
(1)	Modulus:
(1)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(1)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(1)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(1)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(1)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(1)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(1)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(1)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(1)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(1)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(1)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(1)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(1)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(1)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(1)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(1)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(1)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(1)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(1)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(1)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(1)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(1)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(1)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(1)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(1)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(1)	36:d7:77:f5:91:27:08:66:7b:4d
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(1)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	Policy: 2.23.140.1.2.2
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl

(1)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(1)	OCSP - URI:http://ocsp.sectigo.com
(1)Signature	(512 octets)
(1)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(1)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(1)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(1)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(1)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(1)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(1)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(1)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(1)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(1)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(1)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(1)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(1)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(1)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(1)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(1)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(1)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(1)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(1)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(1)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(1)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(1)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(1)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(1)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(1)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(1)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(1)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(1)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(1)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(1)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(1)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(1)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(2)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(2)Valid From	Mar 22 00:00:00 2021 GMT
(2)Valid Till	Jan 18 23:59:59 2038 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:

(2)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(2)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(2)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(2)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(2)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(2)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(2)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(2)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(2)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(2)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(2)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(2)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(2)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(2)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(2)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(2)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(2)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(2)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(2)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(2)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(2)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:
(2)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(2)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(2)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(2)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(2)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(2)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(2)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(2)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(2)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(2)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(2)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(2)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(2)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(2)	7c:6d:cf
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(2)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(2)Signature	(512 octets)
(2)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(2)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(2)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(2)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(2)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43

(2)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(2)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(2)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(2)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(2)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(2)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(2)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(2)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(2)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(2)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(2)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(2)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(2)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(2)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(2)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(2)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(2)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(2)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(2)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(2)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(2)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21
(2)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(2)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(2)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(2)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(2)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(2)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(3)CERTIFICATE 3	
(3)Version	3 (0x2)
(3)Serial Number	01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d
(3)Signature Algorithm	sha384WithRSAEncryption
(3)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)SUBJECT NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(3)Valid From	Feb 1 00:00:00 2010 GMT
(3)Valid Till	Jan 18 23:59:59 2038 GMT
(3)Public Key Algorithm	rsaEncryption
(3)RSA Public Key	(4096 bit)
(3)	RSA Public-Key: (4096 bit)
(3)	Modulus:
(3)	00:80:12:65:17:36:0e:c3:db:08:b3:d0:ac:57:0d:
(3)	76:ed:cd:27:d3:4c:ad:50:83:61:e2:aa:20:4d:09:
(3)	2d:64:09:dc:ce:89:9f:cc:3d:a9:ec:f6:cf:c1:dc:
(3)	f1:d3:b1:d6:7b:37:28:11:2b:47:da:39:c6:bc:3a:
(3)	19:b4:5f:a6:bd:7d:9d:a3:63:42:b6:76:f2:a9:3b:
(3)	2b:91:f8:e2:6f:d0:ec:16:20:90:09:3e:e2:e8:74:

(3)	c9:18:b4:91:d4:62:64:db:7f:a3:06:f1:88:18:6a:
(3)	90:22:3c:bc:fe:13:f0:87:14:7b:f6:e4:1f:8e:d4:
(3)	e4:51:c6:11:67:46:08:51:cb:86:14:54:3f:bc:33:
(3)	fe:7e:6c:9c:ff:16:9d:18:bd:51:8e:35:a6:a7:66:
(3)	c8:72:67:db:21:66:b1:d4:9b:78:03:c0:50:3a:e8:
(3)	cc:f0:dc:bc:9e:4c:fe:af:05:96:35:1f:57:5a:b7:
(3)	ff:ce:f9:3d:b7:2c:b6:f6:54:dd:c8:e7:12:3a:4d:
(3)	ae:4c:8a:b7:5c:9a:b4:b7:20:3d:ca:7f:22:34:ae:
(3)	7e:3b:68:66:01:44:e7:01:4e:46:53:9b:33:60:f7:
(3)	94:be:53:37:90:73:43:f3:32:c3:53:ef:db:aa:fe:
(3)	74:4e:69:c7:6b:8c:60:93:de:c4:c7:0c:df:e1:32:
(3)	ae:cc:93:3b:51:78:95:67:8b:ee:3d:56:fe:0c:d0:
(3)	69:0f:1b:0f:f3:25:26:6b:33:6d:f7:6e:47:fa:73:
(3)	43:e5:7e:0e:a5:66:b1:29:7c:32:84:63:55:89:c4:
(3)	0d:c1:93:54:30:19:13:ac:d3:7d:37:a7:eb:5d:3a:
(3)	6c:35:5c:db:41:d7:12:da:a9:49:0b:df:d8:80:8a:
(3)	09:93:62:8e:b5:66:cf:25:88:cd:84:b8:b1:3f:a4:
(3)	39:0f:d9:02:9e:eb:12:4c:95:7c:f3:6b:05:a9:5e:
(3)	16:83:cc:b8:67:e2:e8:13:9d:cc:5b:82:d3:4c:b3:
(3)	ed:5b:ff:de:e5:73:ac:23:3b:2d:00:bf:35:55:74:
(3)	09:49:d8:49:58:1a:7f:92:36:e6:51:92:0e:f3:26:
(3)	7d:1c:4d:17:bc:c9:ec:43:26:d0:bf:41:5f:40:a9:
(3)	44:44:f4:99:e7:57:87:9e:50:1f:57:54:a8:3e:fd:
(3)	74:63:2f:b1:50:65:09:e6:58:42:2e:43:1a:4c:b4:
(3)	f0:25:47:59:fa:04:1e:93:d4:26:46:4a:50:81:b2:
(3)	de:be:78:b7:fc:67:15:e1:c9:57:84:1e:0f:63:d6:
(3)	e9:62:ba:d6:5f:55:2e:ea:5c:c6:28:08:04:25:39:
(3)	b8:0e:2b:a9:f2:4c:97:1c:07:3f:0d:52:f5:ed:ef:
(3)	2f:82:0f
(3)	Exponent: 65537 (0x10001)
(3)X509v3 EXTENSIONS	
(3)X509v3 Subject Key Identifier	53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(3)X509v3 Key Usage	critical
(3)	Certificate Sign, CRL Sign
(3)X509v3 Basic Constraints	critical
(3)	CA:TRUE
(3)Signature	(512 octets)
(3)	5c:d4:7c:0d:cf:f7:01:7d:41:99:65:0c:73:c5:52:9f
(3)	cb:f8:cf:99:06:7f:1b:da:43:15:9f:9e:02:55:57:96
(3)	14:f1:52:3c:27:87:94:28:ed:1f:3a:01:37:a2:76:fc
(3)	53:50:c0:84:9b:c6:6b:4e:ba:8c:21:4f:a2:8e:55:62
(3)	91:f3:69:15:d8:bc:88:e3:c4:aa:0b:fd:ef:a8:e9:4b
(3)	55:2a:06:20:6d:55:78:29:19:ee:5f:30:5c:4b:24:11
(3)	55:ff:24:9a:6e:5e:2a:2b:ee:0b:4d:9f:7f:f7:01:38
(3)	94:14:95:43:07:09:fb:60:a9:ee:1c:ab:12:8c:a0:9a
(3)	5e:a7:98:6a:59:6d:8b:3f:08:fb:c8:d1:45:af:18:15
(3)	64:90:12:0f:73:28:2e:c5:e2:24:4e:fc:58:ec:f0:f4
(3)	45:fe:22:b3:eb:2f:8e:d2:d9:45:61:05:c1:97:6f:a8
(3)	76:72:8f:8b:8c:36:af:bf:0d:05:ce:71:8d:e6:a6:6f
(3)	1f:6c:a6:71:62:c5:d8:d0:83:72:0c:f1:67:11:89:0c
(3)	9c:13:4c:72:34:df:bc:d5:71:df:aa:71:dd:e1:b9:6c
(3)	8c:3c:12:5d:65:da:bd:57:12:b6:43:6b:ff:e5:de:4d
(3)	66:11:51:cf:99:ae:ec:17:b6:e8:71:91:8c:de:49:fe
(3)	dd:35:71:a2:15:27:94:1c:cf:61:e3:26:bb:6f:a3:67
(3)	25:21:5d:e6:dd:1d:0b:2e:68:1b:3b:82:af:ec:83:67

(3)	85:d4:98:51:74:b1:b9:99:80:89:ff:7f:78:19:5c:79
(3)	4a:60:2e:92:40:ae:4c:37:2a:2c:c9:c7:62:c8:0e:5d
(3)	f7:36:5b:ca:e0:25:25:01:b4:dd:1a:07:9c:77:00:3f
(3)	d0:dc:d5:ec:3d:d4:fa:bb:3f:cc:85:d6:6f:7f:a9:2d
(3)	df:b9:02:f7:f5:97:9a:b5:35:da:c3:67:b0:87:4a:a9
(3)	28:9e:23:8e:ff:5c:27:6b:e1:b0:4f:f3:07:ee:00:2e
(3)	d4:59:87:cb:52:41:95:ea:f4:47:d7:ee:64:41:55:7c
(3)	8d:59:02:95:dd:62:9d:c2:b9:ee:5a:28:74:84:a5:9b
(3)	b7:90:c7:0c:07:df:f5:89:36:74:32:d6:28:c1:b0:b0
(3)	0b:e0:9c:4c:c3:1c:d6:fc:e3:69:b5:47:46:81:2f:a2
(3)	82:ab:d3:63:44:70:c4:8d:ff:2d:33:ba:ad:8f:7b:b5
(3)	70:88:ae:3e:19:cf:40:28:d8:fc:c8:90:bb:5d:99:22
(3)	f5:52:e6:58:c5:1f:88:31:43:ee:88:1d:d7:c6:8e:3c
(3)	43:6a:1d:a7:18:de:7d:3d:16:f1:62:f9:ca:90:a8:fd
(4)CERTIFICATE 4	
(4)Version	3 (0x2)
(4)Serial Number	d2:7f:bb:c1:de:35:9e:52:16:ad:61:49:58:60:99:c4
(4)Signature Algorithm	sha384WithRSAEncryption
(4)ISSUER NAME	
countryName	US
stateOrProvinceName	New Jersey
localityName	Jersey City
organizationName	The USERTRUST Network
commonName	USERTrust RSA Certification Authority
(4)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(4)Valid From	Mar 22 00:00:00 2021 GMT
(4)Valid Till	Jan 18 23:59:59 2038 GMT
(4)Public Key Algorithm	rsaEncryption
(4)RSA Public Key	(4096 bit)
(4)	RSA Public-Key: (4096 bit)
(4)	Modulus:
(4)	00:93:be:d5:36:52:75:d8:01:23:a0:1c:47:42:49:
(4)	ee:63:b6:b7:21:fd:c4:95:d5:48:2b:26:7c:14:53:
(4)	10:da:79:fd:2b:b7:2d:a4:d4:2c:fa:ea:32:dd:49:
(4)	c2:b9:bd:0f:48:3d:7b:5a:98:54:af:9e:5d:31:74:
(4)	4f:07:fc:50:21:dd:a4:cf:68:4f:1b:12:63:6d:25:
(4)	99:4c:2a:99:f3:48:30:61:fa:81:7c:1e:a7:08:4a:
(4)	dc:3e:2b:1c:1f:18:4c:71:aa:35:8c:ad:f8:6e:e8:
(4)	3b:4a:d9:e5:94:02:d6:89:84:13:aa:6d:c8:4f:33:
(4)	cc:50:96:37:92:33:dc:5f:88:e7:9f:54:d9:48:f0:
(4)	98:43:d6:66:fd:9f:17:38:43:c5:01:51:0b:d7:e3:
(4)	23:0f:14:5d:5b:14:e7:4b:be:dd:f4:c8:da:03:37:
(4)	d1:d6:39:a1:21:51:30:83:b0:6d:d7:30:4e:96:5b:
(4)	91:f0:70:24:ab:bf:45:81:64:43:0d:bd:21:3a:2f:
(4)	3c:e9:9e:0d:cb:20:b5:42:27:cc:da:6f:9b:ee:64:
(4)	30:90:39:cd:93:65:81:21:31:b5:23:50:33:37:22:
(4)	e3:38:ed:f8:31:30:cc:45:fe:62:f9:d1:5d:32:79:
(4)	42:87:df:6a:cc:56:19:40:4d:ce:aa:bb:f9:b5:76:
(4)	49:94:f1:27:f8:91:a5:83:e5:06:b3:63:0e:80:dc:
(4)	e0:12:55:80:a6:3b:66:b4:39:87:2d:c8:f0:d0:d1:
(4)	14:e9:e4:0d:4d:0e:f6:5d:57:72:c5:3b:1c:47:56:
(4)	9d:e2:d5:fb:81:61:8c:cc:4d:80:90:34:5b:b7:d7:

(4)	14:75:dc:d8:04:48:9f:c0:c1:28:88:b4:e9:1c:ca:
(4)	a7:b1:f1:56:b7:7b:49:4c:59:e5:20:15:a8:84:02:
(4)	29:fa:38:94:69:9a:49:06:8f:cd:1f:79:14:17:12:
(4)	0c:83:7a:de:1f:b1:97:ee:f9:97:78:28:a4:c8:44:
(4)	92:e9:7d:26:05:a6:58:72:9b:79:13:d8:11:5f:ae:
(4)	c5:38:62:34:68:b2:86:30:8e:f8:90:61:9e:32:6c:
(4)	f5:07:36:cd:a2:4c:6e:ec:8a:36:ed:f2:e6:99:15:
(4)	44:70:c3:7c:bc:9c:39:c0:b4:e1:6b:f7:83:25:23:
(4)	57:d9:12:80:e5:49:f0:75:0f:ef:8d:eb:1c:9b:54:
(4)	28:b4:21:3c:fc:7c:0a:ff:ef:7b:6b:75:ff:8b:1d:
(4)	a0:19:05:ab:fa:f8:2b:81:42:e8:38:ba:bb:fb:aa:
(4)	fd:3d:e0:f3:ca:df:4e:97:97:29:ed:f3:18:56:e9:
(4)	a5:96:ac:bd:c3:90:98:b2:e0:f9:a2:d4:a6:47:43:
(4)	7c:6d:cf
(4)	Exponent: 65537 (0x10001)
(4)X509v3 EXTENSIONS	
(4)X509v3 Authority Key Identifier	keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
(4)X509v3 Subject Key Identifier	56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(4)X509v3 Key Usage	critical
(4)	Digital Signature, Certificate Sign, CRL Sign
(4)X509v3 Basic Constraints	critical
(4)	CA:TRUE
(4)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(4)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(4)X509v3 CRL Distribution Points	
(4)	Full Name:
(4)	URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
(4)Authority Information Access	OCSP - URI:http://ocsp.usertrust.com
(4)Signature	(512 octets)
(4)	3a:6f:04:89:6a:ed:b3:14:d1:c1:43:4f:ff:4f:f7:e0
(4)	6c:80:29:11:81:0b:34:4b:a0:5f:ee:f2:52:95:63:07
(4)	c1:bc:b4:54:6b:f1:09:2d:21:ad:b8:b4:2b:60:48:35
(4)	96:c4:6e:c5:6c:82:94:2a:d3:8e:37:d7:2c:a8:56:7d
(4)	c7:95:da:2b:82:ad:b8:46:57:51:0c:e3:a2:a4:46:43
(4)	4c:50:7d:c0:2f:47:62:dd:6d:84:71:74:d1:77:86:d8
(4)	2f:0a:0b:5a:65:c2:81:33:28:02:21:3e:f7:9f:23:f0
(4)	b7:71:3d:02:7d:35:c9:b8:58:d4:6c:a2:20:4b:08:cd
(4)	8f:0e:98:1e:d2:e0:a3:2f:e1:77:9f:89:2d:49:4b:72
(4)	8f:e0:cc:55:ff:a9:66:d3:ee:d1:2a:b8:e3:18:a6:c3
(4)	4a:59:98:fc:4c:ba:8f:ab:ac:cc:88:6e:0d:6b:a7:de
(4)	11:9b:5e:e9:83:d7:1a:b3:16:95:35:8d:df:8d:6f:0d
(4)	e7:5c:fb:2c:50:a9:2b:a0:ef:d1:c9:51:07:0e:66:ce
(4)	ca:c8:35:b3:b6:66:9e:43:1b:0f:13:8f:54:57:ff:17
(4)	c2:b7:d9:b5:96:98:ca:bb:38:16:90:fd:e1:9e:10:f1
(4)	dc:d7:18:bf:3e:a8:42:63:c6:07:33:6b:b5:ba:3d:13
(4)	9a:0a:5b:9b:6a:f7:75:54:a3:e6:f3:e6:82:5b:be:ee
(4)	ed:2c:69:47:64:c5:18:be:a4:3d:dc:6c:2b:21:62:8e
(4)	97:2e:9d:1e:55:ef:db:14:c9:13:9f:35:dc:e3:ac:07
(4)	05:59:95:ca:f2:c6:db:f4:59:67:c2:e5:46:eb:be:c9
(4)	2e:ff:99:55:35:f9:03:12:ef:5b:93:81:e3:3b:79:b9
(4)	2f:b3:07:ad:b0:27:f5:af:fa:35:c6:02:db:52:01:c2
(4)	5e:73:88:85:80:25:87:46:f7:62:fe:32:68:4b:34:4b
(4)	6b:79:c4:cf:1e:a9:14:8c:dc:95:20:a7:87:4b:b5:c4
(4)	27:8b:71:40:72:a5:28:8f:81:af:16:fb:a3:e4:ba:8c
(4)	90:ab:c5:3d:aa:cf:44:a3:11:b9:36:fa:ef:97:2b:21

(4)	c1:44:bd:ca:f7:19:44:6c:3b:2e:39:71:e2:32:47:fc
(4)	18:48:3d:1f:24:20:10:90:8f:5b:e7:6b:d4:f3:89:93
(4)	ab:c3:53:9f:f2:10:d4:6c:72:85:1b:d3:e6:f0:3a:76
(4)	bd:b8:f3:ff:62:47:df:da:af:c6:c8:4f:29:59:65:19
(4)	fa:be:e6:49:4f:9b:bc:99:45:46:13:88:23:00:6e:ac
(4)	0d:74:bf:e7:b2:a1:76:46:79:f2:a7:9f:17:45:2b:49
(5)CERTIFICATE 5	
(5)Version	3 (0x2)
(5)Serial Number	2c:1a:3c:76:e9:43:dd:dd:ff:19:1b:31:89:0a:ed:71
(5)Signature Algorithm	sha384WithRSAEncryption
(5)ISSUER NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication Root R46
(5)SUBJECT NAME	
countryName	GB
organizationName	Sectigo Limited
commonName	Sectigo Public Server Authentication CA OV R36
(5)Valid From	Mar 22 00:00:00 2021 GMT
(5)Valid Till	Mar 21 23:59:59 2036 GMT
(5)Public Key Algorithm	rsaEncryption
(5)RSA Public Key	(3072 bit)
(5)	RSA Public-Key: (3072 bit)
(5)	Modulus:
(5)	00:a6:43:2d:27:74:74:ea:3a:34:7d:c7:88:d0:ce:
(5)	76:07:b2:be:4f:23:1e:19:cb:f6:05:0e:40:55:cd:
(5)	e3:95:8b:7b:e9:3b:c7:22:ef:e7:35:ed:b6:5b:f4:
(5)	49:5d:7f:6b:59:40:ff:d8:61:3a:18:5e:71:d1:5e:
(5)	1b:b1:8e:ca:dc:87:89:f0:4e:fe:2b:31:bf:4c:66:
(5)	e8:c9:27:c3:bb:e1:79:da:3a:90:05:b6:3a:da:87:
(5)	e1:62:33:1e:88:06:cb:23:4d:be:16:ac:07:78:cf:
(5)	2e:22:b5:2d:71:7f:1b:d9:10:b1:17:7e:7c:4c:1d:
(5)	0d:1d:57:1c:01:76:5c:15:88:19:9d:d6:42:79:7c:
(5)	63:b9:c6:bb:a4:92:76:d0:b2:d4:9d:7b:60:5d:c8:
(5)	c0:13:5b:d8:e1:6b:db:45:e5:b4:5b:a9:a4:79:9c:
(5)	8d:19:d9:a9:4d:c1:6c:e5:8f:ac:cb:2e:8b:b4:4e:
(5)	59:a1:c8:e2:f4:9f:4d:94:d9:d1:7a:8c:76:45:65:
(5)	72:11:7a:40:d4:28:59:e2:0a:8d:f9:9a:55:48:84:
(5)	34:1c:1a:2b:54:56:c1:2b:28:5d:67:21:17:81:98:
(5)	0d:48:db:41:47:0c:6a:c0:8c:c9:78:f2:61:61:de:
(5)	19:52:13:b5:be:4f:bf:b8:fd:e7:c0:39:34:a7:de:
(5)	6a:fe:3e:e7:69:73:42:4a:f1:12:9e:b1:cf:ca:96:
(5)	81:59:12:b4:eb:a9:ca:7c:f4:4f:8b:d9:bd:90:83:
(5)	a1:31:d6:1f:4b:c8:22:15:14:dc:76:02:f6:e1:87:
(5)	22:96:3e:de:70:02:bd:4e:b8:74:55:b8:f0:a2:e2:
(5)	78:58:7f:b1:6e:de:3b:bb:af:19:14:20:ff:69:ce:
(5)	79:23:40:cd:1e:40:a9:68:fa:ee:8f:a7:bd:46:6a:
(5)	fb:2b:8e:b0:64:30:18:5e:e1:00:a8:1e:ed:18:6f:
(5)	e3:77:a2:40:03:e1:f6:3b:8e:02:57:df:0d:46:c5:
(5)	36:d7:77:f5:91:27:08:66:7b:4d
(5)	Exponent: 65537 (0x10001)
(5)X509v3 EXTENSIONS	
(5)X509v3 Authority Key Identifier	keyid:56:73:58:64:95:F9:92:1A:B0:12:2A:04:62:79:A1:40:15:88:21:49
(5)X509v3 Subject Key Identifier	E3:66:74:BB:70:68:8D:2C:5D:4E:0E:A6:4A:8F:9B:37:22:9C:82:92
(5)X509v3 Key Usage	critical

(5)	Digital Signature, Certificate Sign, CRL Sign
(5)X509v3 Basic Constraints	critical
(5)	CA:TRUE, pathlen:0
(5)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(5)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(5)	Policy: 2.23.140.1.2.2
(5)X509v3 CRL Distribution Points	
(5)	Full Name:
(5)	URI:http://crl.sectigo.com/SectigoPublicServerAuthenticationRootR46.crl
(5)Authority Information Access	CA Issuers - URI:http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.p7c
(5)	OCSP - URI:http://ocsp.sectigo.com
(5)Signature	(512 octets)
(5)	05:95:d6:0c:75:82:dd:cb:9b:6f:f7:b5:23:59:33:8b
(5)	c9:4f:16:22:bf:65:4a:07:d3:db:9f:99:53:ab:73:93
(5)	9b:60:7f:d7:2a:45:94:7b:14:8f:a9:19:30:28:52:ab
(5)	ee:bf:0e:b8:6f:a9:ed:53:41:f2:b8:9f:5f:ab:a8:a6
(5)	a2:80:82:cb:d9:b5:9b:2a:ee:20:05:c3:4e:13:a3:ab
(5)	cd:73:17:81:b7:51:2e:b2:1d:dc:43:86:fc:9d:b4:11
(5)	31:02:c2:86:01:00:ab:08:6e:5e:9f:4f:e3:c4:f8:40
(5)	40:52:92:c6:1a:bf:bf:9a:16:33:72:4a:c2:d8:94:fc
(5)	cd:a9:53:37:44:dc:2f:05:db:e9:ea:f8:03:b4:6c:1c
(5)	c6:52:90:65:5b:ae:35:52:1a:a1:8c:a5:b3:cb:30:87
(5)	10:de:48:72:a9:45:dc:51:6a:e4:cb:67:ea:65:fb:01
(5)	af:cb:4a:67:ac:b1:09:19:2c:fd:98:e1:26:7d:ba:1d
(5)	7b:f5:e8:a5:1d:8d:1a:a6:87:27:a6:c8:8f:2c:4f:bb
(5)	a5:2d:c9:01:88:db:a1:27:ed:40:04:a3:30:02:ac:7c
(5)	f4:e8:dc:76:8d:30:18:f4:4e:8d:78:1e:97:ba:86:c4
(5)	c0:b2:b4:db:96:51:9a:f8:25:71:44:46:d4:1a:d5:db
(5)	8b:46:1c:74:e0:c4:27:bc:33:7a:06:96:95:12:31:32
(5)	90:d9:d9:20:96:36:55:62:df:a0:29:d1:6d:58:42:d9
(5)	32:e4:5d:8b:e5:f7:5e:ca:d1:f0:b1:73:f9:a2:d4:88
(5)	34:5f:42:a8:66:c3:74:71:8c:8c:95:2a:fb:ee:f5:43
(5)	d8:63:59:ec:bf:16:26:16:75:12:78:cf:b6:ab:5c:ff
(5)	88:f5:2b:cb:ec:43:63:d3:02:eb:e2:21:95:e2:93:d3
(5)	de:15:29:d1:55:a7:b2:d7:1f:8d:be:c2:f5:3e:d7:b9
(5)	51:a2:54:36:98:ad:8d:fe:70:4b:54:1c:1a:22:18:9b
(5)	41:7c:38:55:82:b0:07:ce:81:73:a7:92:ea:2a:ac:73
(5)	de:0a:12:00:ff:53:85:6c:8e:68:1f:84:af:97:a7:83
(5)	4c:f9:56:33:4d:36:b7:41:e5:77:a7:cc:4e:33:47:30
(5)	ab:5a:7c:a1:91:40:f8:e0:5c:cf:71:58:5a:90:c8:7b
(5)	98:f4:35:62:a5:c3:d8:57:b1:3c:8f:63:f1:de:65:45
(5)	79:f5:a9:2c:91:23:92:45:29:83:7d:ef:30:24:33:d7
(5)	e7:cb:81:f7:fe:e5:b9:dd:06:df:1d:29:c5:00:1c:7d
(5)	f3:f4:6b:22:9a:bc:dc:03:4f:0e:14:7c:9d:f8:70:4c

Appendix

Hosts Scanned (IP)

172.40.123.5

Target distribution across scanner appliances

ANPSGLQUAL01 : 172.40.123.5

Options Profile

Option_Profile_Search_Full

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	On
Close Vulnerabilities on Dead Hosts Count:	Off
Purge old host data when OS changes:	On
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Maximum Scan Duration per Asset:	
Maximum Scan Duration Per Asset:	Disabled
Authentication:	
Windows:	Enabled
Unix/Cisco/Network SSH:	Enabled
Unix Least Privilege Authentication:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Sybase:	Disabled
Kubernetes:	Disabled

SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled
Neo4j:	Disabled
NGINX:	Disabled
Infoblox:	Disabled
BIND:	Disabled
Cisco_APIC:	Disabled
Cassandra:	Disabled
MarkLogic:	Disabled
DataStax:	Disabled
NSX:	Disabled
OLVM:	Disabled
Overall Performance:	High
Allow Parallel Scanning:	Disabled
Limit Per Host CGI Checks:	disabled
Configure Scan for Limited Connectivity:	disabled
Set Maximum Targets per Slice:	disabled
Skip Pre-scanning:	disabled
Additional Certificate Detection:	
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	On
External Scanners:	20
Scanner Appliances:	50
Processes to Run in Parallel:	
Total Processes:	20
HTTP Processes:	20
Packet (Burst) Delay:	Short
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Enabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings	
Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP Off
Ignore firewall-generated TCP RST packets:	On
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	On
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
----------	-------	-------------

Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
 1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
 2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
 3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

CONFIDENTIAL AND PROPRIETARY INFORMATION.

Qualys provides its Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2026, Qualys, Inc.