INFORME FALLA EN AUTENTICACIÓN LDAP

Resumen

Luego de la actualización del controlador de dominio a una versión reciente de Windows Server, el sistema desarrollado en PHP dejó de autenticar usuarios mediante LDAP.

Tras la revisión y análisis del equipo técnico de ITS, se determinó que la causa no estuvo en el código de la aplicación, sino en cambios en los niveles de seguridad del servicio de directorio, particularmente en la forma en que se manejan las conexiones cifradas y la validación de certificados digitales.

1. Análisis

El equipo técnico de ITS llevó a cabo un proceso completo de revisión, diagnóstico, corrección y verificación del método de autenticación. Y se encontró que antes de la actualización, el sistema funcionaba utilizando LDAP en el puerto 389, en algunos casos sin cifrado o con cifrado opcional con el estándar STARTTLS. En ese escenario, la validación del certificado no era estricta, por lo que la autenticación se realizaba sin inconvenientes.

Después de la actualización, el comportamiento del controlador de dominio cambió en dos aspectos importantes:

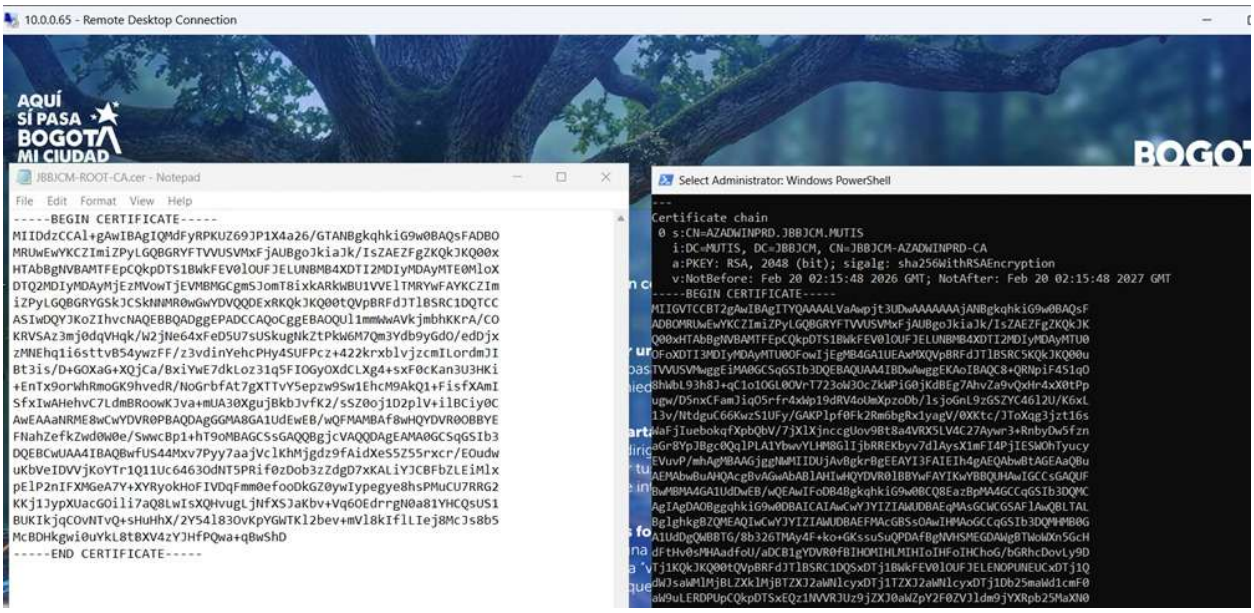
1) Se reforzó la seguridad de las conexiones LDAP, usando cifrando la conexión en el puerto 636.

2) Se volvió más estricta la validación del certificado digital presentado por el servidor, lo que significa que ahora la aplicación debe confiar de manera nombrada y directa del certificado del controlador de dominio.

2. Resumen Técnico

Tras el análisis, el equipo técnico de ITS encontró que al intentar establecer la conexión segura el sistema no lograba validar el certificado del controlador de dominio. Esto se evidenció al realizar pruebas con OpenSSL, donde se observaban errores de validación de certificado.

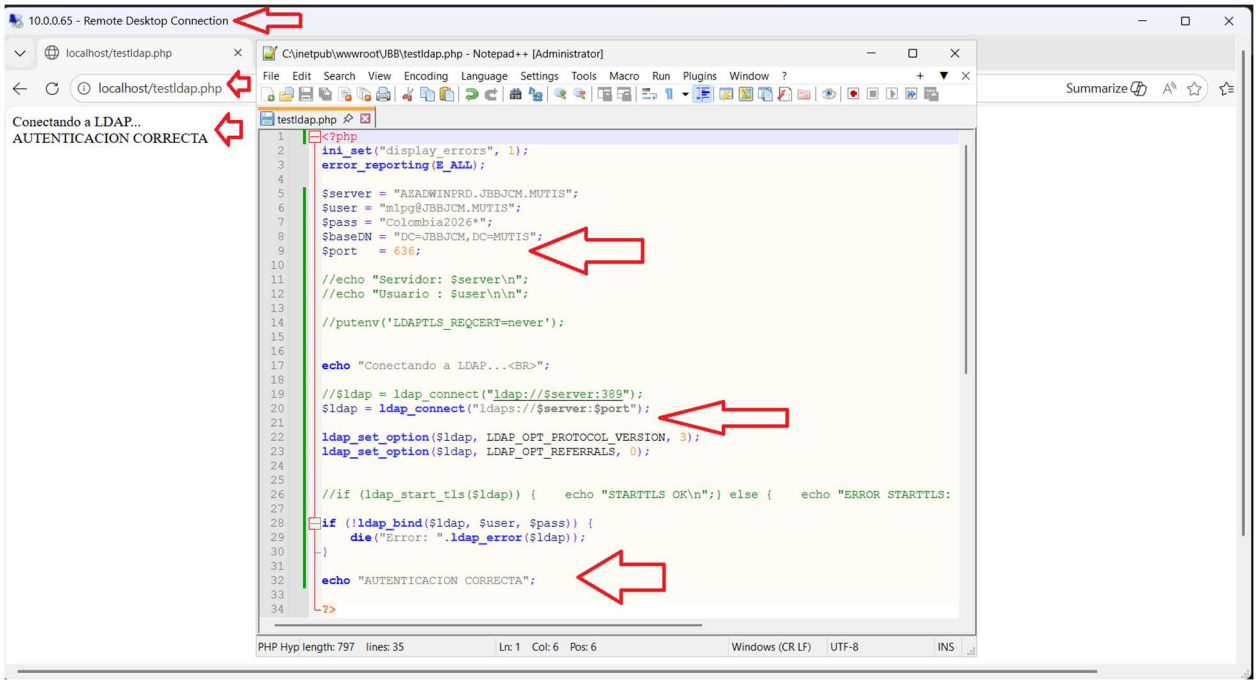
```
Connecting to 10.0.0.57
CONNECTED(000001F8)
depth=0 CN=AZADWINPRD.JBBJCM.MUTIS
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN=AZADWINPRD.JBBJCM.MUTIS
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 CN=AZADWINPRD.JBBJCM.MUTIS
verify return:1
```



ITS SOLUCIONES ESTRATÉGICAS
Calle 37 sur # 33A-75 Piso 2 ▪ Bogotá, Colombia
Tel: (57-1) 478 9209 ▪ FAX: (57-1) 704 5350

contactenos@its-solutions.net
www.its-solutions.net
www.its-solutions.com
www.sw.co

Por lo anterior, el servidor de aplicaciones no podía verificar que el certificado del controlador fuera confiable, porque el certificado no se identificaba registrado en el entorno que utiliza la aplicación y no era reconocido así estuviera instalado. Aunque el certificado ya se encontraba instalado a nivel del sistema operativo en trusted root, la librería utilizada por PHP no lo estaba tomando en cuenta automáticamente como normalmente lo hace, sino que lo reconocía intermitentemente, como se muestra en la prueba realizada:



3. Trabajo realizado

Para restablecer la autenticación, se reinstaló todo el site en un nuevo servidor y posterior a eso se configuró explícitamente en el código de la aplicación la ruta al certificado CA del controlador de dominio.

Con este ajuste:

- La conexión segura pudo validar correctamente el certificado
- LDAPS (puerto 636) comenzó a funcionar sin errores

- LDAP sobre 389 con TLS también funcionó correctamente

Lo anterior, confirma que el problema estaba relacionado exclusivamente con la validación con el certificado del controlador y no con el protocolo LDAP en sí o con fallas en la aplicación.

4. Estado actual

Actualmente, el sistema se encuentra operando correctamente bajo conexiones seguras, utilizando:

- LDAPS con el puerto 636
- LDAP con el puerto 389 con TLS (Deshabilitado, pero se soporta sin problema)

En ambos casos, la autenticación es exitosa siempre que se valide correctamente el certificado del servidor.

5. Conclusiones

La incidencia fue consecuencia directa del fortalecimiento en las políticas de seguridad tras la actualización del controlador de dominio, lo cual es consistente con las prácticas necesarias de protección de servicios de autenticación y conexión con el controlador de dominio.

El sistema no presentaba fallas propias, sino que funcionaba bajo otros criterios de seguridad que ya no son aceptados con la actualización de infraestructura reciente.

La solución aplicada permitió adaptar la aplicación a estos nuevos requerimientos, asegurando la continuidad del servicio de autenticación.