Boletín de alerta

Boletín Nro.:
Fecha de publicación: 25/08/2026
Tema: Actualización de seguridad: RCE Critico en Oracle Weblogic activamente explotado
Traffic Light Protocol (TLP): White

CISA incorporó nuevamente CVE-2026-21962 a su catálogo de vulnerabilidades explotadas activamente, confirmando ataques contra instancias vulnerables de Oracle HTTP Server y Oracle WebLogic Server Proxy Plug-in. La falla, con severidad crítica (CVSS 10.0), permite que un atacante remoto y no autenticado aproveche un control de acceso indebido para obtener acceso no autorizado a información crítica mediante HTTP.

Las organizaciones que utilicen las versiones afectadas —12.2.1.4.0, 14.1.1.0.0 y 14.1.2.0.0— deben tratar esta situación como prioritaria: aplicar el parche publicado por Oracle en su actualización de enero de 2026, limitar la exposición externa de los servicios mientras se completa la remediación y revisar registros para identificar posibles accesos o solicitudes anómalas.

Producto(s) afectado(s):

Los componentes afectados incluyen:
• Versiones de Oracle HTTP Server y Oracle WebLogic Server Proxy Plug-in (Apache):
o 12.2.1.4.0
o 14.1.1.0.0
o 14.1.2.0.0
• Complemento proxy de Oracle WebLogic Server para IIS versión 12.2.1.4.0

Descripción

Se ha reportado una vulnerabilidad crítica no autenticada que afecta a Oracle HTTP Server y al complemento de proxy de Oracle WebLogic Server para Apache e IIS. Al enviar solicitudes HTTP especialmente diseñadas, un atacante remoto puede comprometer el componente proxy sin autenticación. La misma se identificado como CVE-2026-21962 con un score CVSSv3 10.

Una explotación exitosa puede resultar en acceso no autorizado a datos confidenciales y la capacidad de crear, modificar o eliminar datos procesados por el proxy y, potencialmente, por aplicaciones posteriores, lo que representa un riesgo significativo para los entornos empresariales, especialmente las implementaciones con conexión a internet.

Mitigación

• Restrinja la exposición de la red de componentes de servidor proxy y HTTP colocándolos detrás de firewalls, WAF o soluciones VPN/ZTNA, y permita el acceso solo desde redes confiables.

• Revise los registros web y de proxy para detectar patrones de solicitudes sospechosos, puntos finales inesperados o actividad de acceso a datos anormal.

Solución

Aplique de inmediato la actualización del parche crítico de Oracle de enero de 2026 a todas las instalaciones afectadas de Oracle HTTP Server y WebLogic Proxy Plug-in, priorizando los sistemas conectados a Internet.

En el siguiente enlace podrá encontrar información de como proceder con la actualización de su sistema:

https://support.oracle.com/support/?documentId=KA1396

https://www.oracle.com/security-alerts/cpujan2026.html#AppendixFMW

Información adicional:

- https://www.redlegg.com/blog/security-bulletin-oracle-proxy-components-vulnerable-to-unauthenticated-attack
- https://www.oracle.com/security-alerts/cpujan2026.html