Boletín de alerta

Boletín Nro.:
Fecha de publicación: 24/01/2025
Tema: Alerta 2025-09-Vulnerabilidad crítica en Oracle WebLogic Server
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- WebLogic 12.2.1.4.0
- WebLogic 14.1.1.0.0

Descripción

Oracle ha emitido una alerta crítica para abordar la vulnerabilidad CVE-2025-21535, detectada en WebLogic Server. Con un puntaje CVSS de 9.8, esta falla permite a atacantes remotos no autenticados ejecutar código arbitrario (RCE) en sistemas vulnerables.

La vulnerabilidad se origina debido al filtrado insuficiente de datos entrantes en los protocolos T3 e IIOP. Si cualquiera de estos protocolos está habilitado, un atacante podría enviar solicitudes especialmente diseñadas para explotar esta falla y comprometer el sistema.

WebLogic Server es ampliamente utilizado en entornos empresariales debido a sus capacidades avanzadas para la ejecución de aplicaciones Java EE, incluyendo:

1. Servicios web y contenedores EJB.
2. Colas de mensajes JMS.
3. Gestión de transacciones.

Esta vulnerabilidad pone en riesgo infraestructuras críticas al posibilitar la ejecución remota de código malicioso, lo que podría derivar en pérdida de datos, control del sistema o interrupciones en servicios esenciales.

Solución

- Oracle ha lanzado parches para corregir las vulnerabilidades identificadas en WebLogic Server. Se recomienda encarecidamente descargar e instalar la actualización lo antes posible para garantizar la protección de los sistemas afectados. Es necesario contar con una cuenta de licencia de software original para acceder al parche.

- También puede deshabilitar los protocolos **T3** e **IIOP** si no son necesarios.

Información adicional:

- https://www.oracle.com/security-alerts/cpujan2025.html
- https://securityonline.info/cve-2025-21535-cvss-9-8-vulnerability-in-oracle-weblogic-server-could-lead-to-remote-code-execution/
- https://nsfocusglobal.com/oracle-weblogic-server-remote-code-execution-and-denial-of-service-vulnerability-cve-2025-21535-cve-2025-21549/