BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-57
Fecha de publicación: 22/10/2024
Tema: Vulnerabilidad crítica en Oracle WebLogic Server
Traffic Light Protocol (TLP): White

Producto(s) afectado:

Oracle WebLogic Server

- Versiones 12.2.1.4 y 14.1.1.0

Descripción

Una nueva vulnerabilidad crítica identificada como **CVE-2024-21216,** con una puntuación **CVSS de 9.8**, afecta a múltiples versiones de Oracle WebLogic Server, plataforma de servidor de aplicaciones basada en Java ampliamente utilizada, y su explotación permite a atacantes remotos ejecutar código arbitrario sin autenticación.

Esta vulnerabilidad permite a un atacante con acceso simple a la red explotar el servidor WebLogic a través de los protocolos T3 e IIOP, ambos habilitados de forma predeterminada en una instalación estándar de WebLogic, por lo que al ser explotada se puede tener control total del servidor comprometido sin necesidad de interacción del usuario.

Además, Oracle ha lanzado recientemente su actualización de parches críticos de Octubre 2024, que aborda 329 vulnerabilidades, entre las cuales destacan por su criticidad e importancia las siguientes:

1. **CVE-2024-21274 (CVSS de 7.5):** Vulnerabilidad que permite la ejecución remota de código (RCE) en Oracle WebLogic Server a través de un fallo en la validación de entradas, lo que podría ser aprovechado por atacantes remotos sin autenticación.

2. **CVE-2024-21215 (CVSS de 7.5):** Esta vulnerabilidad permite ataques de inyección de código. Un atacante puede enviar solicitudes maliciosas que pueden comprometer el servidor, permitiendo la ejecución de código arbitrario.

3. CVE-2024-21234 (CVSS de 7.5): Esta vulnerabilidad podría permitir la escalada de privilegios en sistemas Oracle WebLogic Server, proporcionando acceso privilegiado a atacantes que ya tienen acceso limitado al sistema.

4. CVE-2024-21260 (CVSS de 7.5): Vulnerabilidad de denegación de servicio (DoS), donde un atacante remoto podría causar la interrupción del servicio en servidores WebLogic, afectando la disponibilidad de las aplicaciones web.

Solución

Oracle ha lanzado parches de seguridad para mitigar esta vulnerabilidad. Es fundamental que los administradores de sistemas actualicen de inmediato a las versiones corregidas para prevenir ataques, ya que la explotación de esta vulnerabilidad puede resultar en una total toma de control del sistema. Las actualizaciones están disponibles en el sitio de soporte de Oracle.

Información adicional:

- https://securityonline.info/cve-2024-21216-cvss-9-8-oracle-weblogic-flaw-that-could-give-attackers-full-control/?&web_view=true
- https://blogs.oracle.com/ebstech/post/critical-patch-update-for-october-2024-now-available
- http://support.oracle.com/rs?type=doc&id=2484000.1

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com