

Boletín de alerta

Boletín Nro.: 106

Fecha de publicación: 21/09/2026

Tema: Alerta 2026-106 RCE en Oracle WebLogic Server — CVE~~2026~~70757

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Oracle identifica estas versiones soportadas como afectadas:

Producto	Componente	Versiones afectadas
Oracle WebLogic Server	Core	12.2.1.4.0
Oracle WebLogic Server	Core	14.1.1.0.0
Oracle WebLogic Server	Core	14.1.2.0.0
Oracle WebLogic Server	Core	15.1.1.0.0

La disponibilidad exacta del parche, número de *patch* y prerequisites deben confirmarse en **My Oracle Support (MOS)**, utilizando el Critical Patch Update de septiembre de 2026 y la matriz de parches correspondiente al entorno.

Descripción

Se identificó una vulnerabilidad crítica en el componente **Core** de Oracle WebLogic Server, parte de Oracle Fusion Middleware. La falla tiene una puntuación **CVSS 9.8 identificado como CVE 2026 70757** y permite que un atacante remoto no autenticado, con acceso de red a los protocolos **T3** o **IIOP**, comprometa completamente una instancia vulnerable de WebLogic Server.

La vulnerabilidad fue corregida como parte del **Oracle Critical Patch Update (CPU) de septiembre de 2026**. No se requiere autenticación, interacción de usuario ni condiciones complejas de explotación; por tanto, deben priorizarse los servidores WebLogic que tengan T3, IIOP, consolas administrativas o aplicaciones expuestas a Internet o accesibles desde redes no confiables.

Solución

La remediación definitiva consiste en aplicar el parche correspondiente del **Oracle Critical Patch Update de septiembre de 2026** para CVE~~2026~~70757. La descarga de parches y los pasos detallados de instalación

están disponibles para clientes autorizados a través de **My Oracle Support**.

<https://support.oracle.com/signin>

No se identifica una mitigación que elimine por completo la vulnerabilidad. El bloqueo de T3/IOP, la deshabilitación de IOP no utilizado y los filtros de conexión reducen temporalmente la superficie de ataque, pero no reemplazan el parche oficial.

Después de actualizar, validar que:

1. El inventario de dominios WebLogic tenga el parche aplicado.
2. Los puertos T3/IOP solo estén disponibles para fuentes autorizadas.
3. La consola administrativa no esté expuesta directamente a Internet.
4. Las aplicaciones y *datasources* operen correctamente tras el reinicio.
5. Se hayan revisado cambios no autorizados y posibles señales de explotación previa.

Información adicional:

- <https://www.oracle.com/security-alerts/cspusep2026.html>
- <https://www.oracle.com/security-alerts/cspusep2026verbose.html>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-70757>
- <https://www.ionix.io/threat-center/cve-2026-70757/>