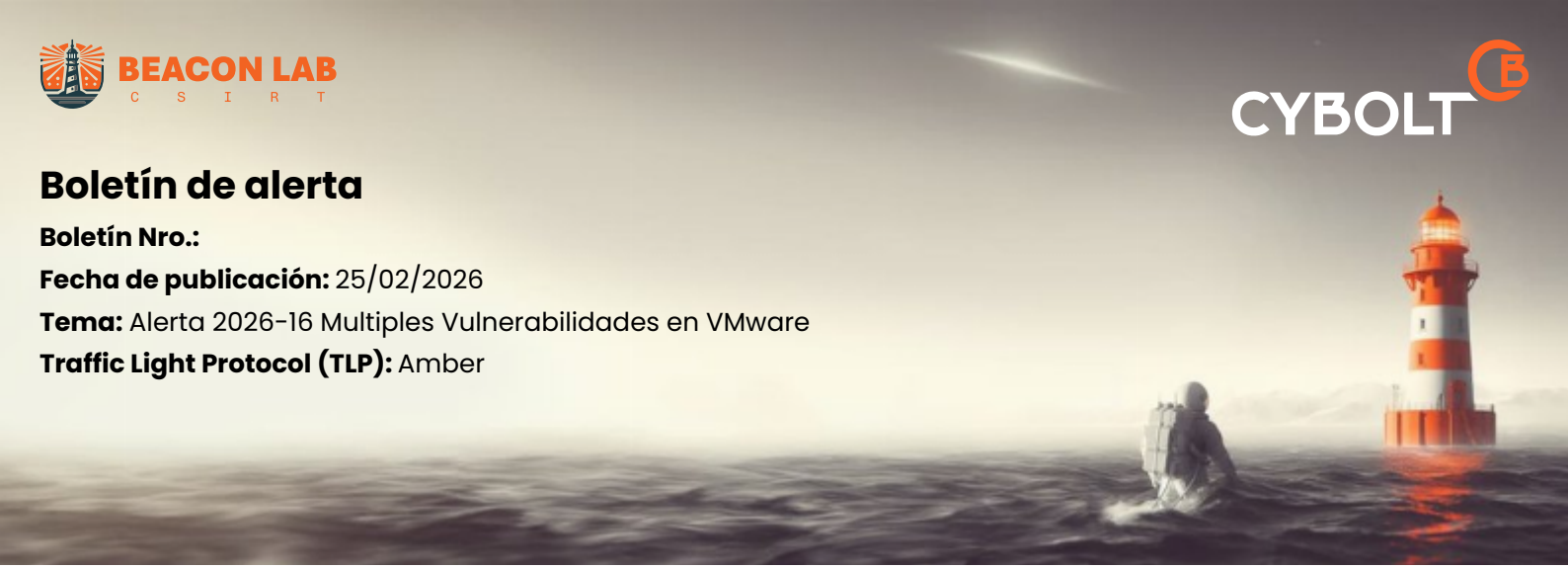

# Boletín de alerta

**Boletín Nro.:**
**Fecha de publicación:** 25/02/2026
**Tema:** Alerta 2026-16 Multiples Vulnerabilidades en VMware
**Traffic Light Protocol (TLP):** Amber

## Producto(s) afectado(s):

- VMware Cloud Foundation Operations, versiones 9.x anteriores a 9.0.2.0.
- VMware Aria Operations, versiones 8.x anteriores a 8.18.6.
- VMware Cloud Foundation (Aria Operations), versiones 5.x y 4.x.
- VMware Telco Cloud Platform y Telco Cloud Infrastructure (Aria Operations).

## Descripción

Broadcom publicó el aviso de seguridad VMSA-2026-0001 el 24 de febrero de 2026, que aborda tres vulnerabilidades críticas en VMware Aria Operations que podrían permitir la ejecución remota de código, el uso de scripts entre sitios y la escalada de privilegios.

Estas fallas afectan a productos clave como VMware Cloud Foundation y las plataformas Telco Cloud, por lo que se insta a las organizaciones a aplicar parches de inmediato. Los problemas tienen puntuaciones CVSS de 6,2 a 8,1, clasificadas como de gravedad importante.

La falla más grave, CVE-2026-22719, es una vulnerabilidad de inyección de comandos en VMware Aria Operations con una puntuación base CVSSv3 de 8,1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

Atacantes maliciosos no autenticados pueden explotarla durante las migraciones de productos asistidas por soporte técnico para ejecutar comandos arbitrarios, lo que provoca la ejecución remota completa de código. Existe una solución alternativa a través de KB430349, pero se recomienda actualizar a versiones corregidas.

CVE-2026-22720 implica secuencias de comandos entre sitios (XSS) almacenadas con una puntuación CVSS de 8,0 (AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H), lo que permite a usuarios con privilegios crear puntos de referencia personalizados para inyectar scripts para acciones administrativas.

No hay ninguna solución alternativa disponible; es esencial implementar parches. CVE-2026-22721 es un problema de escalada de privilegios (CVSS 6.2: AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:L) donde los actores con privilegios de vCenter pueden obtener acceso de administrador en Aria Operations, lo que también

requiere parches sin soluciones alternativas.

## Mitigaciones y soluciones

Los usuarios afectados deben actualizar a las siguientes versiones:

| Producto | Componente | Version afectada | Version corregida |
|---|---|---|---|
| VMware Cloud Foundation | VMware vSphere Foundation / Operations | 9.x | 9.0.2.0 [techdocs.broadcom.com] |
| VMware Aria Operations | N/A | 8.x | 8.18.6 [techdocs.broadcom.com] |
| VMware Cloud Foundation | VMware Aria Operations | 5.x, 4.x | KB92148 |
| VMware Telco Cloud Platform | VMware Aria Operations | 5.x, 4.x | KB428241 |
| VMware Telco Cloud Infrastructure | VMware Aria Operations | 3.x, 2.x | KB428241 |

Se recomienda descargar parches de los portales de soporte de Broadcom y supervisar los entornos durante las migraciones. Priorizar estas actualizaciones previene posibles infracciones en las operaciones de la nube empresarial.

## Información adicional:

- https://www.securityweek.com/vmware-aria-operations-vulnerability-could-allow-remote-code-execution/
- https://www.sdxcentral.com/news/vmware-cloud-management-platform-in-triple-threat/
- https://www.hkcert.org/security-bulletin/vmware-products-multiple-vulnerabilities_20260225
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947