Boletín de alerta

Boletín Nro.: 79
Fecha de publicación: 29/07/2026
Tema: Alerta 2026-79 Vulnerabilidades Críticas en Vmware vCenter, ESXi, Workstation y Fusion
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **VMware vCenter Server**

9.1.x (corregido en 9.1.0.0300)

9.0.x (corregido en 9.0.2.0100)

8.0.x (corregido en 8.0)

7.0.x (afectado; las correcciones únicamente estarán disponibles para clientes con contrato de Extended Support).

- **VMware ESXi**

9.1.x (corregido en 9.1.0.0200)

9.0.x (corregido en 9.0.2.0100)

8.0.x (corregido en 8.0)

7.0.x (afectado; Broadcom indica que los parches podrán obtenerse mediante Extended Support).

- **VMware Workstation Pro**

25H2 (corregido al actualizar a 26H1).

- **VMware Fusion**

25H2 (corregido al actualizar a 26H1).

Descripción

Broadcom, a través del VMware Security Response Center (vSRC), publicó el aviso **VMSA-2026-0006**, el cual corrige cinco vulnerabilidades de seguridad que afectan a VMware vCenter Server, ESXi, Workstation y Fusion. Tres de ellas fueron clasificadas como críticas (CVSS hasta 9.8) debido a que permiten comprometer componentes esenciales de la infraestructura de virtualización, mientras que las dos restantes presentan impacto importante sobre la confidencialidad y la trazabilidad de eventos de seguridad. Hasta el momento de la publicación no existían evidencias públicas de explotación activa, aunque Broadcom recomienda aplicar las actualizaciones con prioridad. A continuación se describen las vulnerabilidades más críticas:

CVE-2026-59309 (CVSS 9.8) – Authentication Bypass en VMware vCenter

Una falla en VMware Directory Service (vmdir) permite que un atacante con acceso a la red pueda eludir el mecanismo de autenticación de vCenter Server y obtener acceso no autorizado al sistema sin necesidad de credenciales válidas. Debido a que vCenter constituye el punto central de administración de infraestructuras VMware, la explotación de esta vulnerabilidad podría comprometer por completo la plataforma de virtualización.

CVE-2026-59310 (CVSS 9.8) – Remote Code Execution mediante Directory Traversal

Esta vulnerabilidad reside en el servidor Syslog de VMware vCenter y combina una condición de Directory Traversal que puede derivar en ejecución remota de código (RCE). Un atacante no autenticado con acceso de red podría ejecutar código arbitrario sobre el servidor vCenter, obteniendo control del sistema y facilitando movimientos laterales dentro del entorno virtualizado.

CVE-2026-47876 (CVSS 9.3) – Escape de máquina virtual en ESXi

Afecta al adaptador de red virtual VMXNET3 mediante una vulnerabilidad de escritura fuera de límites (Out-of-Bounds Write). Un atacante que consiga privilegios administrativos dentro de una máquina virtual podría escapar del entorno virtual y ejecutar código directamente sobre el host ESXi. Esta vulnerabilidad únicamente afecta a máquinas virtuales que utilizan el adaptador VMXNET3, uno de los más empleados en entornos VMware por su alto rendimiento.

Solución:

Broadcom publicó actualizaciones de seguridad para todas las plataformas afectadas mediante el boletín **VMSA-2026-0006**, enlace en el cual se pueden encontrar los parches oficiales. La principal recomendación consiste en actualizar inmediatamente vCenter Server, ESXi, VMware Workstation y VMware Fusion a las versiones corregidas indicadas en la matriz de respuesta del fabricante.

En el caso de CVE-2026-47876, es recomendable identificar las máquinas virtuales que utilizan el adaptador VMXNET3, ya que únicamente ellas son susceptibles a esta vulnerabilidad. No obstante, Broadcom aclara que no es necesario actualizar VMware Tools, ya que la corrección se encuentra en el hipervisor y no en el sistema operativo invitado.

Asimismo, se recomienda restringir el acceso administrativo a vCenter, segmentar adecuadamente las redes de administración, limitar la exposición de los servicios de gestión únicamente a redes confiables y

monitorear cualquier intento de acceso anómalo mientras se implementan las actualizaciones.

Información adicional:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017?ref=darkwebinformer.com
- https://www.broadcom.com/support/vmware-services/security-response
- https://darkwebinformer.com/broadcom-patches-critical-vmware-flaws-enabling-vcenter-authentication-bypass-and-esxi-vm-escape/