

Aviso ID:	59
Fecha del reporte:	30/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades críticas en VMware vCenter y VMware ESX (VMSA-2026-0006): omisión de autenticación, ejecución remota de código y escape de máquina virtual
Herramienta de detección	N/A – Aviso del fabricante y monitoreo de fuentes abiertas
Activos involucrados:	Infraestructura de virtualización: VMware vCenter, VMware ESX, VMware Cloud Foundation, VMware vSphere Foundation, VMware Workstation y VMware Fusion
Tipo de alerta:	Aviso de vulnerabilidad
Nivel de riesgo:	Crítico

Objetivo:

El CSIRT Salud informa a las entidades de su comunidad sobre la publicación del aviso de seguridad VMSA-2026-0006 por parte de Broadcom, mediante el cual se remedian cinco vulnerabilidades que afectan a VMware ESX, VMware vCenter, VMware Workstation y VMware Fusion. Tres de ellas son de severidad crítica y habilitan, respectivamente, la omisión de autenticación en vCenter, la ejecución de código arbitrario en vCenter y el escape de máquina virtual desde un sistema huésped hacia el hipervisor ESX.

El presente aviso tiene carácter preventivo y de remediación. Su propósito es documentar el alcance técnico de las vulnerabilidades, identificar los productos y versiones afectadas, entregar los elementos necesarios para que cada entidad determine su exposición y establecer las recomendaciones de remediación priorizada. Se advierte que, al cierre de este documento,

el fabricante no ha reportado explotación activa en entornos reales, pero tampoco ha publicado medidas de mitigación alternativas para las vulnerabilidades críticas de vCenter, por lo que la aplicación de los parches constituye la única vía de remediación efectiva.

Descripción de las vulnerabilidades:

El 29 de julio de 2026, Broadcom publicó el aviso VMSA-2026-0006, calificado en su conjunto con severidad crítica y con puntajes individuales que oscilan entre 2.7 y 9.8 sobre la escala CVSS v3.1. Las vulnerabilidades fueron reportadas de manera privada al fabricante y remediadas mediante parches acumulativos. El detalle es el siguiente:

CVE	CVSS	Severidad	Descripción	Producto afectado
CVE-2026-59309	9.8	Crítica	Omisión de autenticación en el VMware Directory Service	VMware vCenter
CVE-2026-59310	9.8	Crítica	Recorrido de directorios en el servidor Syslog que permite ejecución de código arbitrario	VMware vCenter
CVE-2026-47876	9.3	Crítica	Escritura fuera de límites en el adaptador de red virtual VMXNET3 (escape de máquina virtual)	VMware ESX
CVE-2026-41703	7.6	Alta	Lectura fuera de límites que puede derivar en divulgación de información o denegación de servicio	VMware ESX, Workstation y Fusion
CVE-2026-41709	2.7	Baja	Registro insuficiente de eventos: permite ejecutar operaciones sin dejar traza en los logs	VMware ESX

CSIRTSALUD-AV-20260730-59

TLP: CLEAR

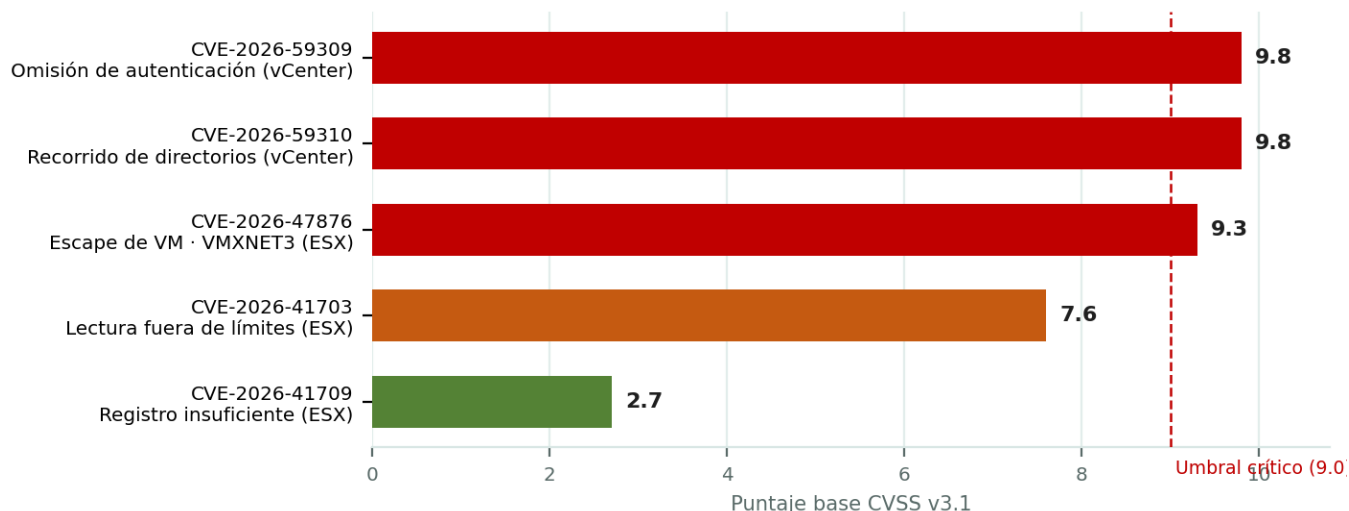


Figura 1. Distribución de severidad (CVSS v3.1) de las cinco vulnerabilidades remediadas en el aviso VMSA-2026-0006.
 Fuente: elaboración propia del CSIRT Salud con base en el aviso del fabricante.

CVE-2026-59309 — Omisión de autenticación en vCenter (CVSS 9.8)

La vulnerabilidad reside en el VMware Directory Service (vmdir), componente responsable de los servicios de directorio y de la autenticación del Single Sign-On de vCenter. Un actor malicioso con acceso de red al servicio puede enviar solicitudes especialmente diseñadas para omitir los controles de autenticación y obtener acceso no autorizado al sistema, sin necesidad de credenciales válidas ni de interacción del usuario.

El impacto recae directamente sobre el plano de administración de la virtualización: un acceso no autorizado a vCenter puede traducirse en control amplio del inventario de máquinas virtuales, almacenes de datos, redes virtuales y hosts ESX asociados. Broadcom atribuye el reporte a Phil Brass y Matt South, de Atredis Partners.

CVE-2026-59310 — Recorrido de directorios en el servidor Syslog de vCenter (CVSS 9.8)

Corresponde a una vulnerabilidad de recorrido de directorios (directory traversal) en el servidor Syslog de vCenter. Un actor malicioso con acceso de red al servicio puede manipular rutas para acceder o escribir en ubicaciones no previstas del sistema de archivos y, a partir de ello, lograr la ejecución de código arbitrario.

CSIRTSALUD-AV-20260730-59**TLP: CLEAR**

En combinación con la vulnerabilidad anterior se configura una cadena de ataque particularmente crítica: acceso inicial sin autenticación seguido de ejecución de código sobre el componente central de administración, lo que convierte a vCenter en una plataforma idónea para el movimiento lateral dentro del centro de datos.

CVE-2026-47876 — Escape de máquina virtual mediante VMXNET3 (CVSS 9.3)

Se trata de una escritura fuera de límites (out-of-bounds write) en el adaptador de red virtual VMXNET3 de VMware ESX. Un actor malicioso que ya cuente con privilegios administrativos locales dentro de una máquina virtual que utilice este adaptador puede ejecutar código en el host ESX subyacente. Broadcom caracteriza expresamente esta condición como un escape de máquina virtual.

Es importante precisar que, aunque VMXNET3 cuenta con un controlador dentro del sistema operativo huésped, la vulnerabilidad se localiza en el lado de ESX y se remedia exclusivamente mediante la actualización del hipervisor. La actualización de VMware Tools o de los controladores del huésped no mitiga esta vulnerabilidad, si bien el fabricante recomienda mantener dichos componentes actualizados como práctica de mantenimiento rutinario.

El escenario de riesgo más relevante para las entidades es la ruptura del aislamiento entre cargas de trabajo: el compromiso de una única máquina virtual podría escalar hacia el hipervisor y, desde allí, afectar la totalidad de las máquinas virtuales alojadas en el mismo host.

CVE-2026-41703 y CVE-2026-41709 — Vulnerabilidades complementarias

CVE-2026-41703 (CVSS 7.6) es una lectura fuera de límites que un actor con privilegios de despliegue de máquinas virtuales puede provocar, con potencial de divulgación de información o de generar una condición de denegación de servicio sobre el proceso del host. En VMware Workstation y VMware Fusion el impacto se limita a divulgación de información, con severidad baja (CVSS 2.7). El reporte se atribuye a Maxim Suhanov.

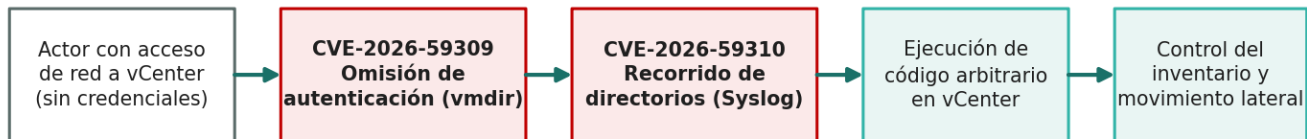
CVE-2026-41709 (CVSS 2.7) corresponde a un registro insuficiente de eventos en VMware ESX que permitiría a un administrador malicioso ejecutar determinadas operaciones sin que

CSIRTSALUD-AV-20260730-59

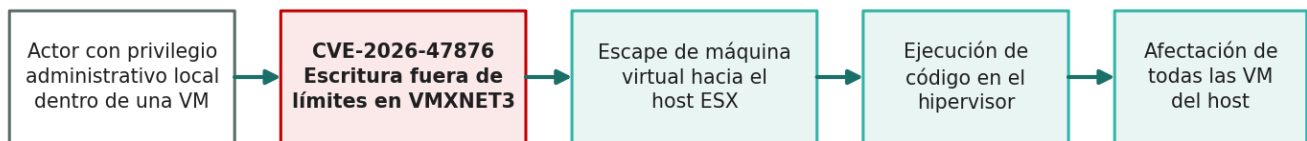
TLP: CLEAR

estas queden registradas en los logs del sistema. Aunque su severidad es baja, tiene implicaciones directas sobre la trazabilidad y la capacidad de auditoría e investigación forense. El reporte se atribuye a Ian Barton, de CrowdStrike.

Vía A · Plano de administración (VMware vCenter)



Vía B · Hipervisor (VMware ESX) — escape de máquina virtual



Escenario posterior común: cifrado masivo de almacenes de datos (ransomware sobre hipervisores), exfiltración de información clínica e indisponibilidad de servicios misionales

Productos y versiones afectadas:

Las vulnerabilidades afectan a VMware ESX, VMware vCenter, VMware Workstation y VMware Fusion. Por extensión, resultan afectados todos los productos que incorporan ESX o vCenter, incluyendo VMware Cloud Foundation, VMware vSphere Foundation, VMware Telco Cloud Platform y VMware Telco Cloud Infrastructure. Las versiones corregidas son las siguientes:

Producto / versión	CVE	CVSS	Versión corregida
Cloud Foundation y vSphere Foundation 9.1.x.x (vCenter)	CVE-2026-59309, CVE-2026-59310	9.8	9.1.0.0300
Cloud Foundation y vSphere Foundation 9.0.x.x (vCenter)	CVE-2026-59309, CVE-2026-59310	9.8	9.0.2.0100

CSIRTSALUD-AV-20260730-59

TLP: CLEAR

Producto / versión	CVE	CVSS	Versión corregida
VMware vCenter 8.0	CVE-2026-59309, CVE-2026-59310	9.8	8.0 U3k
VMware Cloud Foundation 5.x (vCenter)	CVE-2026-59309, CVE-2026-59310	9.8	Parche asíncrono a 8.0 U3k
Cloud Foundation y vSphere Foundation 9.1.x / 9.0.x (ESX)	CVE-2026-47876	9.3	ESXi-9.1.0.0200-25557999 / ESXi- 9.0.2.0100-25595025
VMware ESX 8.0	CVE-2026-47876	9.3	ESXi80U3k-25595708
Cloud Foundation y vSphere Foundation (ESX)	CVE-2026-41703	7.6	ESXi-9.1.0.0-25370933 / ESXi- 9.0.2.0100-25595025
VMware ESX 8.0	CVE-2026-41703	7.6	ESXi80U3i-25205845
VMware Cloud Foundation 5.2.x	CVE-2026-41703	7.6	5.2.3
VMware Workstation 25H2 y VMware Fusion 25H2	CVE-2026-41703	2.7	26H1
Cloud Foundation y vSphere Foundation (ESX)	CVE-2026-41709	2.7	ESXi-9.1.0.0-25370933 / ESXi- 9.0.2.0100-25595025
VMware ESX 8.0	CVE-2026-41709	2.7	ESXi80U3j-25429389

Consideraciones sobre la aplicación de parches

- **Parches acumulativos.** El fabricante precisa que los parches son acumulativos, es decir, la versión vigente incorpora todas las correcciones previamente publicadas. Si bien CVE-2026-59309 se corrigió inicialmente en la versión 9.1.0.0200, la versión 9.1.0.0300 es la más reciente disponible e incluye dicha corrección.
- **Restricción en la ruta de actualización de vCenter 8.0.** Las notas de versión de vCenter 8.0 Update 3k advierten que la actualización desde 8.0 U3k hacia vCenter 9.1.0, o hacia cualquier parche basado en 9.1.0, no está soportada actualmente; la ruta hacia 9.1.x estará disponible en una versión futura. Este aspecto debe considerarse en la planeación de mantenimiento.

- **Entornos Telco Cloud.** Las entidades que operen VMware Telco Cloud Platform o Telco Cloud Infrastructure deben consultar el artículo de conocimiento KB449886 del fabricante para la guía específica de remediación.
- **Ausencia de mitigaciones alternativas.** No se han publicado soluciones temporales para las vulnerabilidades críticas de vCenter, por lo que la actualización es la única vía de remediación disponible.

Estado de explotación y contraste de fuentes:

El CSIRT Salud contrastó el aviso del fabricante con reportes especializados y con la documentación técnica oficial, con corte al 29 de julio de 2026. Los resultados de esa verificación se resumen a continuación:

- **Fuente primaria oficial.** El origen de la información es el aviso VMSA-2026-0006 publicado por Broadcom, complementado por el documento de preguntas frecuentes del repositorio oficial de VMware y por las notas de versión de los productos afectados.
- **Sin evidencia de explotación en el momento de la publicación.** El fabricante manifiesta que las vulnerabilidades fueron reportadas de manera privada y que no dispone de información que sugiera explotación en entornos reales. Se indica que el documento de preguntas frecuentes será actualizado conforme se disponga de nueva información.
- **Cobertura independiente coincidente.** Medios y portales especializados en seguridad reprodujeron el contenido del aviso sin reportar casos de explotación activa, y coinciden en señalar la ausencia de mitigaciones alternativas y la necesidad de priorizar el parcheo de las instancias de vCenter alcanzables desde la red.
- **Sin prueba de concepto pública identificada.** A la fecha de este documento no se identificó código de explotación público asociado a los identificadores CVE relacionados.

En consecuencia, el CSIRT Salud clasifica el evento como VULNERABILIDAD CONFIRMADA POR EL FABRICANTE, SIN EVIDENCIA DE EXPLOTACIÓN ACTIVA. No obstante, la

infraestructura de virtualización VMware ha sido objetivo recurrente de actores de ransomware y de grupos de espionaje, y el intervalo entre la publicación de un aviso crítico de vCenter o ESXi y la aparición de pruebas de concepto o de explotación oportunista ha sido históricamente breve. La divulgación pública del aviso incrementa el interés de actores maliciosos sobre estos componentes, por lo que la ventana de remediación debe considerarse limitada.

Análisis de riesgo para el sector salud:

La infraestructura de virtualización constituye la capa de soporte sobre la cual operan los sistemas de información en salud, las bases de datos institucionales, los servicios de autenticación y, en muchas entidades, los propios servidores de respaldo. Un compromiso del hipervisor o de su plano de administración no afecta a un sistema aislado, sino de manera simultánea a todas las cargas de trabajo alojadas, con impacto directo sobre la continuidad de la prestación del servicio.

A esto se suma que la remediación de estas vulnerabilidades exige ventanas de mantenimiento sobre componentes críticos, lo que en la práctica tiende a dilatar la aplicación de parches. Esa dilación es precisamente la condición que los actores de ransomware han aprovechado de forma sistemática en campañas dirigidas contra hipervisores, en las que el cifrado se ejecuta directamente sobre los almacenes de datos y afecta de manera irreversible múltiples máquinas virtuales en una sola acción.

Riesgos derivados para las entidades

- **Compromiso del plano de administración.** Acceso no autorizado a vCenter con posibilidad de creación, modificación, clonación o eliminación de máquinas virtuales que soportan sistemas de información en salud.
- **Ruptura del aislamiento entre cargas de trabajo.** El escape de máquina virtual permite que el compromiso de un único sistema huésped se propague hacia el hipervisor y hacia las demás máquinas virtuales del mismo host.

CSIRTSALUD-AV-20260730-59

TLP: CLEAR

- **Despliegue de ransomware sobre hipervisores.** El acceso al plano de administración habilita el cifrado masivo de almacenes de datos y la afectación de copias de respaldo alojadas en la misma infraestructura.
- **Exposición de datos sensibles de salud.** Acceso o exfiltración de información clínica y datos personales, con las implicaciones correspondientes frente a la Ley 1581 de 2012 y los deberes de notificación asociados.
- **Interrupción de la prestación del servicio.** Indisponibilidad de sistemas misionales, historia clínica electrónica, servicios de autenticación o componentes de interoperabilidad.
- **Pérdida de trazabilidad.** El registro insuficiente de eventos (CVE-2026-41709) dificulta la detección temprana y la investigación forense posterior a un incidente.

Mapeo MITRE ATT&CK

Técnica	Nombre	Táctica	Relación
T1190	Exploit Public-Facing Application	Acceso inicial	CVE-2026-59309 / CVE-2026-59310
T1210	Exploitation of Remote Services	Movimiento lateral	CVE-2026-59309 / CVE-2026-59310
T1212	Exploitation for Credential Access	Acceso a credenciales	CVE-2026-59309 (vmmdir / SSO)
T1068	Exploitation for Privilege Escalation	Escalada de privilegios	CVE-2026-47876
T1611	Escape to Host	Escalada de privilegios	CVE-2026-47876 (escape de VM)
T1562.008	Impair Defenses: Disable or Modify Cloud Logs	Evasión de defensas	CVE-2026-41709
T1499.004	Endpoint Denial of Service: Application or System Exploitation	Impacto	CVE-2026-41703
T1082	System Information Discovery	Descubrimiento	CVE-2026-41703
T1486	Data Encrypted for Impact	Impacto	Escenario posterior asociado a ransomware sobre hipervisores

Verificación de versiones e identificación de activos expuestos:

Las entidades pueden emplear los siguientes comandos y consultas para inventariar sus activos VMware y determinar su nivel de exposición. Su ejecución debe realizarse por personal autorizado y conforme a los procedimientos internos de gestión de cambios.

Identificación de versión de vCenter y ESX

```
# Versión y build de ESX (consola SSH o ESXi Shell del host)
vmware -vl
esxcli system version get

# Versión y build de vCenter Server (shell del appliance)
vpxd -v
cat /etc/vmware/.buildInfo

# Inventario de versiones desde PowerCLI
Connect-VIServer -Server <vcenter-fqdn>
Get-VMHost | Select-Object Name, Version, Build, ConnectionState | Sort-Object Name
$global:DefaultVIServer | Select-Object Name, Version, Build
```

Identificación de máquinas virtuales con adaptador VMXNET3

```
# Máquinas virtuales que utilizan el adaptador vulnerable (CVE-2026-47876)
Get-VM | Get-NetworkAdapter | Where-Object { $_.Type -eq "Vmxnet3" } |
  Select-Object @{N="VM";E={$_.Parent.Name}}, Name, Type, NetworkName |
  Sort-Object VM | Export-Csv .\inventario_vmxnet3.csv -NoTypeInformation
```

Verificación de exposición de la interfaz de administración

- Confirmar que los puertos de administración de vCenter (TCP 443 y 5480) y de ESX (TCP 443 y 902) no sean accesibles desde Internet ni desde segmentos de usuario final; el plano de administración debe residir en un segmento dedicado con acceso restringido mediante listas de control de acceso.

- Validar en la superficie de ataque externa, mediante las herramientas de gestión de superficie expuesta disponibles, que no existan instancias de vCenter o ESX publicadas hacia Internet.
- Revisar reglas de publicación, VPN, NAT y accesos de terceros o proveedores que puedan habilitar alcance de red hacia vCenter desde redes no confiables.

Monitoreo y detección:

Adicionalmente a la remediación, se recomienda reforzar el monitoreo de los siguientes elementos, con especial atención a los sistemas que no puedan ser actualizados de forma inmediata:

- **Registros de autenticación de vCenter.** Revisar los logs de los servicios de directorio y Single Sign-On (por ejemplo, /var/log/vmware/vmdird/, /var/log/vmware/sso/ y websso.log) en búsqueda de autenticaciones exitosas sin evento previo de solicitud de credenciales, sesiones desde direcciones IP no habituales o accesos fuera del horario institucional.
- **Registros del servicio Syslog y del servidor web de vCenter.** Identificar solicitudes con secuencias de recorrido de directorios, rutas codificadas o intentos de escritura en ubicaciones no previstas del sistema de archivos.
- **Actividad sobre los hosts ESX.** Monitorear la habilitación no autorizada de SSH o del ESXi Shell, la creación de usuarios locales, tareas programadas inusuales, modificación de archivos de configuración y reinicios inesperados de procesos del hipervisor.
- **Comportamiento en las máquinas virtuales.** A través de la solución EDR institucional, priorizar detecciones de escalada de privilegios locales y de manipulación de controladores en servidores virtualizados, dado que el privilegio administrativo local es la condición previa para explotar CVE-2026-47876.

- **Integridad de la auditoría.** Verificar que los hosts ESX y vCenter remitan sus registros hacia la plataforma de correlación institucional y que no existan interrupciones o vacíos en el envío, considerando la vulnerabilidad de registro insuficiente (CVE-2026-41709).

Recomendaciones para las entidades:

El CSIRT Salud recomienda a las entidades de la comunidad adoptar, en la medida de sus capacidades y de acuerdo con su modelo de operación tecnológica, las siguientes acciones:

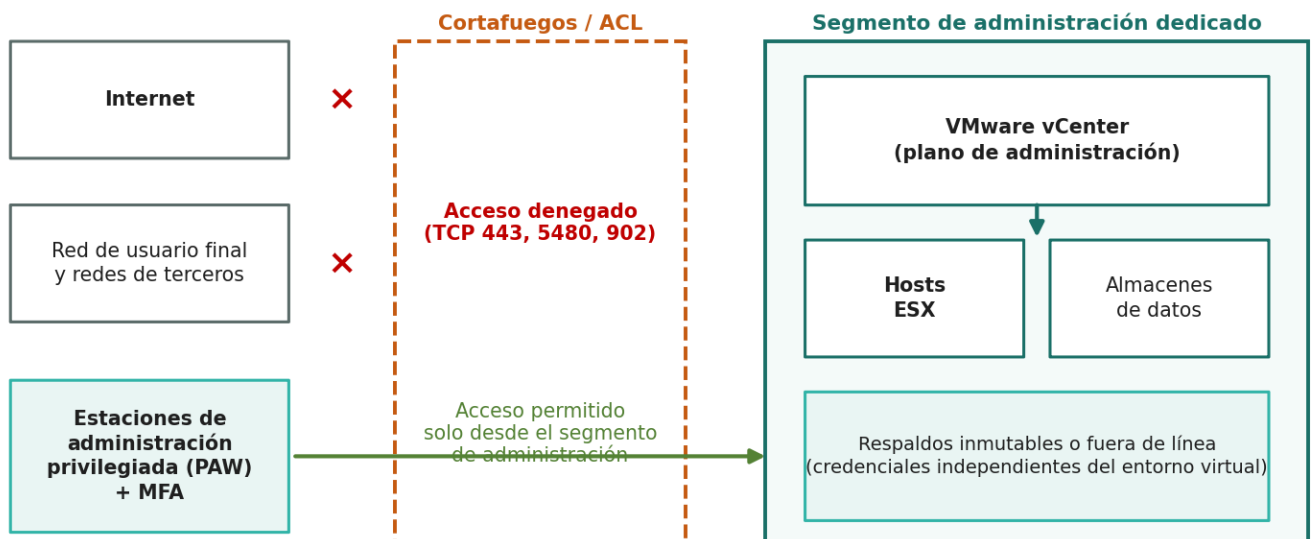
Remediación y gestión de parches

- **Inventariar los activos afectados.** Identificar todas las instancias de VMware vCenter, VMware ESX, VMware Cloud Foundation, vSphere Foundation, Workstation y Fusion en operación, registrando versión y número de compilación, así como su ubicación en la arquitectura de red.
- **Aplicar los parches de manera prioritaria.** Actualizar vCenter a las versiones 9.1.0.0300, 9.0.2.0100 u 8.0 U3k según corresponda, y los hosts ESX a las compilaciones señaladas en este documento, dentro de la ventana de mantenimiento más próxima. Al no existir mitigaciones alternativas para las vulnerabilidades críticas de vCenter, la actualización debe tratarse como acción prioritaria del proceso de gestión de vulnerabilidades.
- **Priorizar las instancias con mayor exposición.** Atender en primer lugar los sistemas vCenter accesibles desde Internet, desde redes de terceros o desde segmentos de usuario final, así como los hosts ESX que alojen sistemas misionales o información sensible de salud.
- **Verificar la ruta de actualización antes de ejecutar el cambio.** Considerar la restricción documentada por el fabricante respecto a la actualización desde vCenter 8.0 U3k hacia versiones 9.1.x, y validar la compatibilidad con los demás componentes del entorno antes de programar la intervención.

- **Actualizar VMware Workstation y VMware Fusion.** Migrar las instalaciones 25H2 a la versión 26H1 en las estaciones de trabajo institucionales, y mantener actualizados VMware Tools y los controladores del sistema operativo huésped como práctica de mantenimiento, sin perjuicio de que estas actualizaciones no remedian CVE-2026-47876.

Reducción de la superficie de exposición

- **Restringir el acceso al plano de administración.** Confinar el acceso a vCenter y ESX a un segmento de administración dedicado, con autenticación multifactor, estaciones de administración privilegiada y listas de control de acceso explícitas; eliminar cualquier publicación directa de estos servicios hacia Internet.



- **Depurar cuentas y privilegios.** Revisar las cuentas con privilegios sobre vCenter y ESX, desactivar las que correspondan a personal retirado o a terceros sin vinculación vigente y limitar los perfiles con capacidad de despliegue y modificación de máquinas virtuales.
- **Validar la integridad y el aislamiento de las copias de respaldo.** Comprobar la existencia de respaldos recientes y verificados de vCenter, de la configuración de los hosts y de las máquinas virtuales críticas, preferiblemente con copias inmutables o fuera de línea que no dependan de credenciales del entorno virtualizado.

Monitoreo, reporte y escalamiento

- **Reforzar el monitoreo durante el periodo de exposición.** Aplicar las medidas de detección descritas en este documento mientras se completa el despliegue de los parches.
- **Documentar y reportar.** Registrar las acciones de remediación en el sistema de gestión de la entidad e informar al CSIRT Salud el estado de aplicación de los parches, así como cualquier hallazgo o dificultad técnica identificada durante el proceso, con el fin de facilitar la coordinación sectorial.
- **Escarar ante indicios de compromiso.** En caso de identificar accesos no autorizados, actividad anómala en el plano de administración o cualquier evidencia de explotación, activar el procedimiento interno de gestión de incidentes y notificar de manera inmediata al CSIRT Salud para el acompañamiento correspondiente.

Referencias

- Broadcom (29 de julio de 2026). VMSA-2026-0006: VMware ESX, vCenter, Workstation, and Fusion updates address multiple vulnerabilities. Disponible en support.broadcom.com.
- VMware / Broadcom. Preguntas frecuentes del aviso VMSA-2026-0006, repositorio oficial vcf-security-and-compliance-guidelines. Disponible en github.com/vmware.
- Broadcom. VMware vCenter 8.0 Update 3k Release Notes. Disponible en techdocs.broadcom.com.
- Broadcom. KB449886: VMware Telco Cloud response to VMSA-2026-0006. Disponible en knowledge.broadcom.com.
- The Hacker News (29 de julio de 2026). Three Critical VMware Flaws Allow Auth Bypass, Code Execution, and VM Escape. Disponible en thehackernews.com.
- SecurityWeek (29 de julio de 2026). Critical VM Escape Vulnerability Patched in VMware ESXi. Disponible en securityweek.com.

CSIRTSALUD-AV-20260730-59**TLP: CLEAR**

- Security Affairs (29 de julio de 2026). Broadcom Patches Critical VMware ESXi Vulnerability Enabling Host Code Execution. Disponible en securityaffairs.com.
- Cyber Security News (29 de julio de 2026). Critical VMware vCenter Flaws Let Remote Attackers Bypass Authentication and Execute Code. Disponible en cyberpress.org.

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con este aviso de vulnerabilidad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **contacto@csirtsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

