Alerta de

Seguridad

Vulnerabilidades Críticas Detectadas en VMware

COLCERT AL-20250722-068

TLP:CLEAR

Se identificaron múltiples vulnerabilidades críticas en productos **VMware** que plantea un riesgo de escalamiento de privilegios y ejecución de código desde máquinas virtuales comprometidas. Dado que estos entornos son ampliamente usados en infraestructura crítica, existe una alta probabilidad de que actores maliciosos aprovechen estos fallos en campañas dirigidas a entornos corporativos y de nube híbrida. Este análisis busca facilitar decisiones proactivas para mitigar amenazas antes de su explotación a gran escala.

Consolidado de Vulnerabilidades por Severidad

CRITICIDAD	NÚMERO	DESCRIPCIÓN	IMPACTO
Críticas	**3**	Permiten a ciberdelincuentes ejecutar código arbitrario desde una máquina virtual comprometiendo el host.	Captura de información sensible, interrupción de servicios críticos y despliegue de nuevas amenazas en toda la infraestructura.
Alta	**1**	Permite la filtración de información del host a través de vSockets desde una máquina virtual.	Exposición de credenciales, claves o información confidencial utilizada por otros sistemas o servicios.

Vulnerabilidades identificadas

CVE	PRODUCTO	SCORE CVSS	IMPACTO	ACCIONES RECOMENDADAS
CVE-2025-41236	VMware ESXi - versiones 7.0, 8.0 y anteriores. VMware Workstation - 17.x. VMware Fusion - 13.x. VMware Cloud Foundation - 4.5.x, 5.x. VMware Telco Cloud Platform - 2.x, 3.x, 4.x, 5.x.	**9.3**	Permite ejecutar código en el host físico, comprometiendo completamente el hipervisor.	Actualizar a la versión corregida de VMware ESXi, Workstation o Fusion. Si no es posible, evitar el uso del adaptador VMXNET3 en máquinas virtuales no confiables.

CVE	PRODUCTO	SCORE CVSS	IMPACTO	ACCIONES RECOMENDADAS
CVE-2025-41237	VMware ESXi - versiones 7.0, 8.0 y anteriores. VMware Workstation - 17.x. VMware Fusion - 13.x. VMware Cloud Foundation - 4.5.x, 5.x. VMware Telco Cloud Platform - 2.x, 3.x, 4.x, 5.x.	**9.3**	Puede ser explotada para escribir fuera de límites (out-of-bounds write), llevando a ejecución de código arbitrario.	Aplicar los parches oficiales y restringir el uso de funciones VMCI en entornos donde no sea estrictamente necesario.
CVE-2025-41238	VMware ESXi - versiones 7.0, 8.0 y anteriores. VMware Workstation - 17.x. VMware Fusion - 13.x. VMware Cloud Foundation - 4.5.x, 5.x. VMware Telco Cloud Platform - 2.x, 3.x, 4.x, 5.x.	**9.3**	Se puede generar una escritura fuera de límites en la memoria (heap overflow), obteniendo ejecución de código.	Actualizar los productos afectados. Evitar configuraciones no compatibles o personalizadas del controlador PVSCSI.
CVE-2025-41239	VMware Tools en Windows versions 11.x, 12.x, 13.x. VMware ESXi - versiones 7.0, 8.0 y anteriores. VMware Workstation - 17.x. VMware Fusion - 13.x. VMware Cloud Foundation - 4.5.x, 5.x VMware Telco Cloud Platform - 2.x, 3.x, 4.x, 5.x.	7.1	Permite acceder a fragmentos de memoria del host o de otros procesos que se comunican a través de vSockets.	Instalar las actualizaciones de seguridad y, si no se requieren, deshabilitar vSockets para minimizar la superficie de ataque.

¿Cómo se explotan estas vulnerabilidades?

Estas **vulnerabilidades en VMware pueden ser aprovechadas por un ciberdelincuente con privilegios administrativos que tenga acceso a una máquina virtual para tomar el control del servidor principal**. Esto le permitiría acceder a otras máquinas, capturar información confidencial o afectar servicios importantes. Además, una de las fallas podría permitir exfiltrar datos del sistema sin necesidad de control total, solo aprovechando una debilidad en la comunicación interna.

Técnicas MITRE ATT&CK Asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Explotación para ejecución del cliente	T1203	Los adversarios explotan vulnerabilidades en aplicaciones de cliente (como software de virtualización) para ejecutar código arbitrario.
Explotación para escalamiento de privilegios	T1068	Se utilizan fallos en el sistema para obtener permisos más altos de los que el atacante ya tiene. Aquí, se aprovechan desde la VM para alcanzar control sobre el host.
Recolección de datos del sistema local	T1005	El atacante accede y extrae información almacenada localmente. En el caso de CVE-2025-41239, se filtran fragmentos de memoria del host que podrían contener datos sensibles.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Protección contra explotación	M1050	Aplicar los parches oficiales tan pronto sea posible para corregir vulnerabilidades.
Gestión de cuentas privilegiadas	M1026	Limitar privilegios dentro de las máquinas virtuales y en el hipervisor.
Segmentación de red	M1030	Aislar las máquinas virtuales críticas para evitar la propagación hacia los host.

Soluciones y mitigaciones disponibles

- ❑ Aplicar los parches de seguridad publicados por VMware indicados en el boletín VMSA-2025-0013. Estas corrigen directamente las vulnerabilidades críticas y altas en ESXi, Workstation, Fusion y Tools.
- ❑ Para CVE-2025-41236 (VMXNET3) evitar el uso del adaptador VMXNET3 en máquinas virtuales no confiables o con usuarios externos.
- ❑ Para CVE-2025-41237 (VMCI) deshabilitar el canal VMCI si no se necesita para la operación de las VMs.
- ❑ Para CVE-2025-41238 (PVSCSI) revisar que las VMs no estén configuradas con controladores PVSCSI en modos no soportados.
- ❑ Para CVE-2025-41239 (vSockets) deshabilitar vSockets si no son requeridos para las aplicaciones o sistemas internos.

IMPACTO PARA COLOMBIA Y LA REGIÓN

- **Sectores afectados**: gobierno, salud, financiero, educación e infraestructura crítica.
- **Riesgo alto de ciberataques** (ransomware, exfiltración, control del host) desde máquinas virtuales.
- **Consecuencias**: acceso a datos sensibles, caída de servicios y propagación entre máquinas virtuales.
- **Implicaciones en seguridad digital**:
  - Violación de la confidencialidad, integridad y disponibilidad.
  - Posible incumplimiento de normas y regulaciones sectoriales.
  - Riesgo de espionaje.

FUENTES:

Alerta oficial de seguridad (Security Advisory) publicada por Broadcom, empresa propietaria de VMware

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877

Bases de datos y catálogos de vulnerabilidades

NIST National Vulnerability Database (NVD)

https://nvd.nist.gov/vuln/detail/CVE-2025-41236
https://nvd.nist.gov/vuln/detail/CVE-2025-41237
https://nvd.nist.gov/vuln/detail/CVE-2025-41238
https://nvd.nist.gov/vuln/detail/CVE-2025-41239

NIVEL DE RIESGO

ALTO