Alert Bulletin

Bulletin N.: 59
Publication Date: 17/07/2025
Subject: Alerta 2025-59 Múltiples vulnerabilidades en productos de VMware
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Fundación VMware Cloud
- Fundación VMware vSphere
- VMware ESXi
- VMware Workstation Pro
- VMware Fusion
- Herramientas de VMware
- Plataforma de nube VMware Telco
- Infraestructura de nube de VMware Telco

Descripción

Se han reportado varias vulnerabilidades críticas en productos VMWare, 3 de severidad crítica y 1 de severidad alta, cuya explotación podría permitir a un atacante ejecutar código en el *host* o filtrar memoria de los procesos que se comunican con vSockets. Podemos rescastar **CVE-2025-41236** (CVSSv3 9.3) y **CVE-2025-41237 (CVSSv3 9.3)** que afectan a VMware ESXi, Workstation y Fusion, ambos de tipo Out **-of-bounds Write (escritura fuera de los límites**).

A continuación se enumeran las vulnerabilidades en detalle:

- **CVE-2025-41236** : vulnerabilidad de desbordamiento de enteros. Un actor malintencionado con privilegios administrativos locales en una máquina virtual con el adaptador de red virtual VMXNET3, puede aprovechar este problema para ejecutar código en el *host* . Los adaptadores virtuales que no son VMXNET3 no se ven afectados por este problema.

- **CVE-2025-41237** : desbordamiento de enteros en VMCI (Virtual Machine Communication Interface) que conduce a una escritura fuera de límites. Un actor malicioso con privilegios administrativos locales en una máquina virtual, podría explotar esta vulnerabilidad para ejecutar código como proceso VMX de la máquina virtual que se ejecuta en el *host* . En ESXi, la explotación está contenida dentro del *sandbox* VMX mientras que, en Workstation y Fusion, esto puede llevar a la ejecución de

código en la máquina donde están instalados.

- **CVE-2025-41238** : vulnerabilidad de desbordamiento de montón en el controlador PVSCSI (SCSI paravirtualizado) que conduce a una escritura fuera de los límites. Un actor malicioso con privilegios administrativos locales en una máquina virtual, puede explotar este problema para ejecutar código como proceso VMX de la máquina virtual que se ejecuta en el *host* . En ESXi, la explotación está contenida dentro del *sandbox* VMX y sólo es explotable con configuraciones no soportadas. En Workstation y Fusion, esto puede llevar a la ejecución de código en la máquina donde están instalados.

- **CVE-2025-41239** : VMware ESXi, Workstation, Fusion y VMware Tools contienen una vulnerabilidad de divulgación de información debido al uso de una memoria no inicializada en vSockets. Un actor malicioso con privilegios administrativos locales en una máquina virtual podría ser capaz de explotar esta vulnerabilidad para filtrar la memoria de los procesos que se comunican con vSockets.

Para información adicional sobre las vulnerabilidades puede dirigirse al siguiente enlace: https://github.com/vmware/vcf-security-and-compliance-guidelines/tree/main/security-advisories/vmsa-2025-0013

Solución:

Se recomienda aplicar los parches publicados por el fabricante:

- Fundación VMware Cloud, Fundación VMware vSphere
  - ESX
    - Versión corregida **ESXi-9.0.0.0100-24813472**
  - Herramientas de VMware
    - Versión corregida 13.0.1.0
- VMware ESXi
  - **ESXi80U3f-24784735**
  - **ESXi80U2e-24789317**
  - **ESXi70U3w-24784741**
- Estación de trabajo VMware
  - Versión corregida 17.6.4
- VMware Fusion
  - Versión corregida 13.6.4
- VMware Cloud Foundation 5.X
  - Parche asíncrono para **ESXi80U3f-24784735**
- VMware Cloud Foundation 4.5.x
  - Parche asíncrono para **ESXi70U3w-24784741**
- Plataforma de nube VMware Telco
  - 5.x, 4.x
    - Versión Corregida **ESXi80U3f-24784735**
  - 3.x, 2.x
    - Versión Corregida **ESXi70U3w-24784741**

- Herramientas de VMware
    - 13.xx
        - Versión corregida 13.0.1.0
    - 12.xx, 11.xx
        - Versión corregida 12.5.3

Para los enlaces de descarga y actualización puede consultar con el fabricante, para más información sobre el proceso de parcheo, puede dirigirse al siguiente enlace:

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

Información adicional:

- **https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877**
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-vmware-1?sstc=u88504nl570192