Boletín de alerta

Boletín Nro.:
Fecha de publicación: 09/01/2026
Tema: Alerta 2026-03 Explotacion activa de vulnerabilidades 0day en productos VMware
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **VMware ESXi**
- Versiones afectadas: Principalmente **8.0 Update 3** y versiones cercanas

Descripción

Se detectó una campaña de ataques altamente sofisticada en la que actores de amenaza de habla china utilizaron dispositivos **SonicWall VPN previamente comprometidos** como vector de acceso inicial a redes corporativas. Una vez dentro, los atacantes ejecutaron una **cadena avanzada de exploits contra VMware ESXi**, lo que les permitió escapar de máquinas virtuales y obtener control directo sobre el hipervisor, comprometiendo completamente la infraestructura de virtualización.

Durante la intrusión se explotaron **tres vulnerabilidades encadenadas**, las cuales permitieron a los atacantes escalar privilegios, corromper memoria del hipervisor y evadir los mecanismos de aislamiento de las máquinas virtuales, logrando una toma de control total del entorno ESXi.

CVE-2025-22224 – Crítica (CVSS 9.3)

Esta vulnerabilidad permite la **ejecución remota de código directamente en el hipervisor ESXi** mediante una condición de escritura fuera de límites en el componente VMCI. Su explotación permite al atacante ejecutar comandos con privilegios elevados, comprometiendo el host que aloja todas las máquinas virtuales.

CVE-2025-22225 – Alta (CVSS 8.2)

Esta vulnerabilidad permite a un atacante **escapar del entorno de una máquina virtual hacia el kernel del hipervisor**, rompiendo el aislamiento de seguridad entre las VMs y el host. Su explotación facilita el movimiento lateral y la instalación de persistencia a nivel de hipervisor.

CVE-2025-22226 – Media (CVSS 7.1)

Esta vulnerabilidad permite la **filtración de memoria del proceso VMX**, exponiendo información sensible del hipervisor que puede ser utilizada para apoyar la explotación de otras vulnerabilidades y facilitar la evasión de controles de seguridad.

Para consultar la investigación completa y los detalles técnicos del caso, puede revisar el siguiente enlace:

https://www.huntress.com/blog/esxi-vm-escape-exploit

Estas vulnerabilidades permiten a los atacantes tomar control del servidor ESXi, instalar backdoors invisibles, robar o destruir máquinas virtuales, manipular infraestructura crítica y utilizar el hipervisor como punto de pivote para comprometer el resto de la red corporativa. **Aunque las fallas fueron divulgadas públicamente en 2025, investigaciones recientes revelaron que ya estaban siendo explotadas desde al menos 2024**, lo que confirma el uso de ataques tipo zero-day altamente avanzados y resalta la importancia no solo de aplicar las actualizaciones de seguridad, sino también de verificar activamente si existen indicios de compromiso dentro de la red.

Solución:

- **Actualizar de inmediato VMware ESXi** con los parches de seguridad más recientes publicados por el fabricante

Información adicional:

- https://www.huntress.com/blog/esxi-vm-escape-exploit
- https://www.bleepingcomputer.com/news/security/vmware-esxi-zero-days-likely-exploited-a-year-before-disclosure/
- https://www.broadcom.com/support