

Boletín de alerta

Boletín Nro.: 115

Fecha de publicación: 19/10/2026

Tema: Alerta 2026-115 PwnEscape permite atacar al host desde una máquina virtual

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

CVE-2026-99999 afecta código presente en el kernel Linux desde la versión 2.6.27, cuando no se ha incorporado la corrección correspondiente. El escenario principal investigado es un host de virtualización Linux que procesa tráfico IPv4 y metadatos de checksum controlados desde una máquina virtual invitada.

Rama del kernel	Versiones afectadas dentro de la rama, sin el parche	Primera versión corregida
5.10	Hasta 5.10.271	5.10.272
5.15	Hasta 5.15.222	5.15.223
6.1	Hasta 6.1.189	6.1.190
6.6	Hasta 6.6.158	6.6.159
6.12	Hasta 6.12.112	6.12.113
6.18	Hasta 6.18.56	6.18.57
7.2	Hasta 7.2.10	7.2.11

Descripción

PwnEscape, identificada como CVE-2026-99999 (CVSS 9.3), es una vulnerabilidad en la pila de red IPv4 del kernel Linux que permite a un atacante que controla una máquina virtual invitada comprometer el aislamiento respecto del host mediante paquetes con metadatos de checksum manipulados.

La falla está relacionada con la validación de metadatos utilizados para completar el checksum de paquetes IPv4. Un paquete manipulado puede provocar una escritura que modifica el encabezado IPv4 después de que el kernel ya lo haya procesado y validado. En el escenario investigado, estos metadatos proceden de una máquina virtual a través de virtio-net.

Aunque la investigación se centra en un escape de máquinas virtuales KVM, el defecto reside en el kernel Linux y no exclusivamente en KVM. La exposición depende de la versión del kernel, los parches incorporados y la configuración de red y virtualización del host.

Productos y plataformas afectadas

Producto o plataforma	Condición de exposición
Hosts Linux con un kernel vulnerable	Sistemas que procesen paquetes con los metadatos manipulados descritos en la investigación.
Hipervisores Linux con KVM y virtio-net	Hosts que ejecuten máquinas virtuales desde las que un atacante pueda enviar tráfico manipulado hacia la pila de red del anfitrión.
Plataformas de virtualización multiusuario y sandboxes basados en VMs	Mayor riesgo cuando alojan máquinas virtuales de clientes o cargas no confiables sobre infraestructura compartida.
Distribuciones como CloudLinux, AlmaLinux, Ubuntu y Red Hat Enterprise Linux	Validar la afectación y disponibilidad del paquete corregido por versión y variante de kernel en el aviso de cada proveedor.

La investigación reporta filtración de memoria del kernel y una cadena de explotación que logró ejecución de código como root en hosts de laboratorio.

El riesgo es especialmente relevante para hipervisores, plataformas multiusuario y entornos que ejecutan máquinas virtuales no confiables.

Existen correcciones en ramas estables del kernel; su disponibilidad debe verificarse con cada distribución.

Solucion

La solución consiste en instalar el kernel corregido que publique el proveedor para la versión y variante del sistema afectado. Las correcciones se incorporaron en las ramas estables indicadas a continuación; las distribuciones pueden incorporar el parche a sus propios paquetes sin utilizar estos mismos números de versión. Por ello, el aviso del fabricante debe ser la referencia para validar la remediación.

Rama del kernel Versión estable corregida

5.10	5.10.272
5.15	5.15.223
6.1	6.1.190
6.6	6.6.159
6.12	6.12.113
6.18	6.18.57
7.2	7.2.11

Información adicional:

- Investigación técnica de PWN.AI: <https://pwn.ai/blog/pwnescape>

- CloudLinux — mitigación y estado de actualización:
<https://blog.cloudlinux.com/cve-2026-99999-guest-to-host-escape/>
- AlmaLinux — disponibilidad de kernels corregidos:
<https://almalinux.org/blog/2026-10-16-pwnescape-cve-2026-99999/>
- Red Hat — evaluación de la vulnerabilidad:
<https://access.redhat.com/security/cve/cve-2026-99999>
- Ubuntu — estado por paquete y versión:
<https://ubuntu.com/security/CVE-2026-99999>