

Alert Bulletin

Bulletin N.: 115

Publication Date: 19/10/2026

Subject: Alert 2026-115 PwnEscape allows attacking the host from a virtual machine

Traffic Light Protocol (TLP): White

Affected product(s):

CVE-2026-99999 affects code present in the Linux kernel since version 2.6.27, when the corresponding fix has not been incorporated. The main scenario investigated is a Linux virtualization host that processes IPv4 traffic and controlled checksum metadata from a guest virtual machine.

Kernel branch Affected versions within the branch, without the patch First corrected version

5.10	Up to 5.10.271	5.10.272
5.15	Up to 5.15.222	5.15.223
6.1	Up to 6.1.189	6.1.190
6.6	Up to 6.6.158	6.6.159
6.12	Up to 6.12.112	6.12.113
6.18	Up to 6.18.56	6.18.57
7.2	Up to 7.2.10	7.2.11

Description

PwnEscape, identified as CVE-2026-99999 (CVSS 9.3), is a vulnerability in the IPv4 network stack of the Linux kernel that allows an attacker controlling a guest virtual machine to compromise the isolation from the host through packets with manipulated checksum metadata.

The flaw is related to the validation of metadata used to complete the IPv4 packet checksum. A manipulated packet can cause a write that modifies the IPv4 header after the kernel has already processed and validated it. In the investigated scenario, this metadata comes from a virtual machine through virtio-net.

Although the research focuses on a KVM virtual machine escape, the flaw resides in the Linux kernel and not exclusively in KVM. The exposure depends on the kernel version, the patches incorporated, and the host's network and virtualization configuration.

Affected products and platforms

Product or platform	Exposure condition
Linux hosts with a vulnerable kernel	Systems that process packets with the manipulated metadata described in the research.
Linux hypervisors with KVM and virtio-net	Hosts running virtual machines from which an attacker can send manipulated traffic to the host’s network stack.
Multi-user virtualization platforms and VM-based sandboxes	Higher risk when hosting client virtual machines or untrusted workloads on shared infrastructure.
Distributions such as CloudLinux, AlmaLinux, Ubuntu, and Red Hat Enterprise Linux	Validate the impact and availability of the corrected package by version and kernel variant in each vendor’s advisory.

The research reports kernel memory leakage and an exploitation chain that achieved code execution as root on lab hosts.

The risk is especially relevant for hypervisors, multi-user platforms, and environments running untrusted virtual machines.

Fixes exist in stable kernel branches; their availability must be verified with each distribution.

Solution

The solution consists of installing the corrected kernel published by the vendor for the version and variant of the affected system. The fixes were incorporated into the stable branches indicated below; distributions may incorporate the patch into their own packages without using these same version numbers. Therefore, the manufacturer’s advisory should be the reference for validating remediation.

Kernel branch Corrected stable version

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

Additional information:

- Technical research from PWN.AI: <https://pwn.ai/blog/pwnescape>

- CloudLinux — mitigation and update status:
<https://blog.cloudlinux.com/cve-2026-99999-guest-to-host-escape/>
- AlmaLinux — availability of corrected kernels:
<https://almalinux.org/blog/2026-10-16-pwnescape-cve-2026-99999/>
- Red Hat — vulnerability assessment:
<https://access.redhat.com/security/cve/cve-2026-99999>
- Ubuntu — status by package and version:
<https://ubuntu.com/security/CVE-2026-99999>