GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

28 August 2026

Advisory 205: CVE-2026-66384 and CVE-2026-53362_Linux Kernel IPv6 Privilege Escalation Vulnerabilities, One Actively Exploited

Release Date: 27th August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

All organisations operating Linux servers, virtual machines or appliances, regardless of distribution. CERTVU states that the actively exploited vulnerability addressed here affects multiple products including, but not limited to, SUSE, Red Hat and other products built on Linux.

Highest priority should be given to hosts running containers, hosts providing shell accounts to multiple users, and any shared or multi-tenant Linux platform. This advisory should be read together with CERTVU Advisory 201 (CVE-2022-0995), and all three vulnerabilities are best addressed in a single kernel patching exercise.

What is it?

These advisory covers two vulnerabilities in the IPv6 networking subsystem of the Linux kernel. Both permit an unprivileged local user to escalate privileges. They are addressed together because they affect the same subsystem and are resolved by the same remediation.

CVE-2026-66384 was flagged on 27 August 2026 on the basis of confirmed exploitation in the wild.

of low risk, and should disregard any third-party analysis that purports to describe the flaw in detail unless it is corroborated by a distribution vendor.

CVE-2026-53362 is a separate, documented flaw in the same subsystem, published on 4 July 2026, carrying a CVSS v3.1 Base Score of 7.8 and rated by Red Hat as having Important security impact.

CERTVU has not been able to establish from the available information whether these two records describe the same underlying defect, related defects, or entirely distinct ones. That distinction does not affect the action required, as the same kernel update resolves both.

What does this mean?

The documented flaw is a container escape, not merely a privilege escalation.

Red Hat has stated that a user with local access inside a container could escape to the host, bypass SELinux enforcement, and gain system administrator access on the host itself. Containers are frequently relied upon as a security boundary, on the understanding that a compromise inside a container is contained to that container. This removes that assumption.

The practical consequence is that a single compromised containerised application can yield root on the host and, through it, access to every other container running on that host. Where the host forms part of a shared platform, the exposure extends to workloads belonging to other applications, departments or customers.

The kernel is shared between the host and all containers running on it, so updating an individual container image does not address either issue. The host kernel must be updated and the host restarted.

What are the systems affected?

1. Linux kernels containing the vulnerable code paths in the IPv6 networking subsystem, prior to the versions in which the fixes were applied - (Affected)
2. Kernels carrying the upstream fixes or the vendor-backported fixes supplied by the distribution - (Not affected, patched)

Not all distributions and releases are affected by both issues. Some older releases do not contain the vulnerable code at all, and vendors differ in which of their supported releases require an update.

Mitigation process

CERTVU recommends the following:

1. Determine Exposure From Your Distribution Vendor

Check the running kernel version on each host, then confirm against your vendor's advisories for CVE-2026-66384 and CVE-2026-53362 whether that release is affected and which kernel package resolves each issue.

```
uname -r
```

2. Update the Host Kernel and Reboot

Apply the current kernel package supplied by your distribution vendor. A kernel update does not take effect until the system is restarted, so a host that has been patched but not rebooted remains fully exploitable. Verify after rebooting that the running kernel is the updated one.

Other mitigating options include;

- Prioritize Container Hosts and Shared Platforms
- Conduct a Compromise Assessment, Not Only a Patch

- Consider Disabling IPv6 Where It Is Not Required

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://nvd.nist.gov/vuln/detail/CVE-2026-66384
3. https://www.cve.org/CVERecord?id=CVE-2026-53362
4. https://access.redhat.com/security/vulnerabilities/RHSB-2026-009
5. https://ubuntu.com/security/CVE-2026-53362
6. https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk