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

8 October 2025

Advisory 101: Linux Kernel Heap Out-of-Bounds Write Vulnerability

Release Date: 06th of October 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

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

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2021-22555 is a **heap out-of-bounds write** in the Linux kernel's Netfilter implementation (file net/netfilter/x_tables.c) that was disclosed in 2021. The flaw exists in the setsockopt() handling (IPT_SO_SET_REPLACE / IP6T_SO_SET_REPLACE) and allows corruption of heap memory when exploited under certain conditions, leading to privilege escalation or denial-of-service (kernel crash)

What are the Systems affected?

The bug affects Linux kernels since v2.6.19-rc1and was fixed in mainline kernel 5.12 (and backported to a set of stable branches). Any Kernel older than the patched backport levels as potentially vulnerable unless vendor specifiy.

What does this mean?

Successful exploitation can lead to **local privilege escalation to root**, **kernel code execution**, or **DoS** (kernel crash). Because PoCs exist that can bypass typical mitigation techniques, this is considered a high-impact kernel privilege escalation.

This allows an attacker to gain privileged or cause a DoS (via heap memory corruption) through user name space

Mitigation process

CERTVU recommend:

1. Patch – apply vendor kernel updates – Upgrade the Linux kernel / operating system packages to a version that contains the official fix.
2. Disable unprivileged user namespaces, harden local account access (Remove or lock unused local accounts).
3. Apply host hardening: reduce the number of services where untrusted users can run code (e.g., limit SSH access, disable interactive shells for service accounts), and segregate workloads so that untrusted users cannot execute code on machines that must remain unpatched.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2021-22555
3. https://github.com/google/security-research/security/advisories/GHSA-xxx5-8mvq-3528