مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in Linux Kernel

Tracking #:432319208

Date:29-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a privilege escalation vulnerability, CVE-2026-46331, nicknamed "Pedit COW," has been disclosed in the Linux kernel's Traffic Control (tc) subsystem. The vulnerability allows an unprivileged local attacker to obtain full root privileges on vulnerable Linux systems.

TECHNICAL DETAILS:

A Linux kernel vulnerability, CVE-2026-46331, known as "Pedit COW," has been disclosed that allows an unprivileged local attacker to escalate privileges to root by exploiting a flaw in the Linux Traffic Control (tc) subsystem.
The vulnerability resides within the tcf_pedit_act() function of the act_pedit kernel module, where an improper implementation of the Copy-on-Write (COW) mechanism allows corruption of shared page-cache memory instead of private memory pages.
Unlike traditional privilege escalation attacks, Pedit COW modifies only the in-memory cached version of privileged executables (e.g., /bin/su) while leaving the original files on disk untouched, enabling attackers to bypass conventional file integrity monitoring (FIM) and checksum-based detection.
A working proof-of-concept (PoC) exploit was released publicly within 24 hours of the CVE assignment, significantly increasing the risk of exploitation against unpatched Linux systems.

Vulnerability Details:

- CVE ID: CVE-2026-46331
- Vulnerability Name: Pedit COW
- Vulnerability Type: Local Privilege Escalation (LPE)
- Affected Component: Linux Kernel Traffic Control (tc) subsystem
- Affected Module: act_pedit
- Vulnerable Function: tcf_pedit_act()
- Root Cause: Improper implementation of the Copy-on-Write (COW) mechanism, where writable memory validation occurs before runtime packet offsets are fully resolved.
- Underlying Issue: Runtime-calculated packet edit offsets can write beyond the intended private memory page, resulting in corruption of shared page-cache memory.
- Attack Vector: Local access to a vulnerable Linux system.
- Privileges Required: Low (unprivileged local user).
- User Interaction: None required.
- Exploitation Method: Attackers abuse the act_pedit module through Linux Traffic Control (tc) after obtaining namespace-scoped CAP_NET_ADMIN privileges via unprivileged user namespaces.
- Primary Impact: Escalation of privileges from a standard user to full root access.

Confirmed Vulnerable

- Red Hat Enterprise Linux (RHEL) 8
- Red Hat Enterprise Linux (RHEL) 9
- Red Hat Enterprise Linux (RHEL) 10
- Debian 11
- Debian 12
- Debian 13 (Trixie)

- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- Ubuntu 26.04

Temporary Mitigations:

- Restrict unprivileged user namespaces.
- Disable the vulnerable module act_pedit if not used.

RECOMMENDATIONS:

Immediate Actions:

- Apply vendor-supplied kernel updates immediately.
- Reboot systems after installing patched kernels.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2026-46331