CERT-MU Vulnerability Note

Linux flaw with Multiple Point of Contact Exploit

Vulnerability Note: VN-2025-04

Date of Issue: 20 June 2025

Severity Rating: High

Systems Affected:

- Linux Kernel version lower than 6.2

Description

A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system.

This vulnerability (CVE-2023-0386) is trivial to exploit and impacts a wide range of Linux distributions, including popular ones like Debian, Red Hat, Ubuntu, and Amazon Linux, if they are using a vulnerable kernel version.

Solution

Users are advised to upgrade the latest version/
https://security-tracker.debian.org/tracker/CVE-2023-0386

CVE Information

CVE-2023-0386

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,