Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Google Patches Actively Exploited Android Vulnerabilities in September 2025 Update

Vulnerability Note: VN-2025-23

Date of Issue: 03 September 2025

Severity Rating: High

Systems Affected:

- Android devices with security patch level prior to 2025-09-01
- Android devices with security patch level prior to 2025-09-05 (for kernel and vendor components)

Description

Google has addressed multiple security vulnerabilities in its Android operating system, including two high-severity flaws that have been actively exploited in targeted attacks. The most critical issues include privilege escalation vulnerabilities in both the Linux kernel and Android Runtime components.

The first actively exploited vulnerability (CVE-2025-38352) relates to a race condition in the Linux kernel between handle_posix_cpu_timers() and posix_cpu_timer_del() functions. Under certain timing conditions, particularly when tasks exit and timer operations overlap, this bug could be abused to gain elevated privileges or destabilize the system.

The second exploited vulnerability (CVE-2025-48543) affects the Android Runtime and allows a local attacker to gain elevated privileges without requiring user interaction. Exploitation attempts for this vulnerability have been observed in the wild.

Additionally, a critical Remote Code Execution vulnerability (CVE-2025-48539) in the System component could allow an attacker to execute code remotely without user interaction when in proximity to the target device.

CVE Information

CVE-2025-38352
CVE-2025-48543
CVE-2025-48539

Mitigation

Google has recommended that users apply the latest security updates immediately. Devices updated to the 2025-09-05 patch level are protected against all vulnerabilities listed in this month's

bulletin. Users should check for and install available security updates through their device settings and ensure automatic updates are enabled for optimal protection.

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