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

13 March 2026

Advisory 120: Qualcomm Multiple Chipsets Memory Corruption Vulnerability

Release Date: 03rd March 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

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-2026-21385 is a high-severity vulnerability (CVSS 7.8) affecting the graphics subsystem of certain Android devices that use Qualcomm chipsets. The flaw exists in the Qualcomm Adreno GPU graphics driver, which is responsible for handling graphics processing and memory allocation.

The vulnerability results from an integer overflow (CWE-190) during memory allocation calculations. When the system incorrectly calculates the required memory buffer size, it can lead to memory corruption, allowing data to overflow into restricted memory areas.

What are the systems affected?

The vulnerability impacts Android devices using Qualcomm chipsets, specifically those that rely on the Qualcomm graphics component within the Android ecosystem.

See more affected Products (in Product Status).

Affected environments include:

- Android smartphones and tablets using Qualcomm Snapdragon chipsets.
- Devices using the Qualcomm Adreno GPU driver within the Android graphics stack.
- Android builds prior to the March 2026 Android security patch level.

The flaw potentially affects hundreds of device models and more than 200 Qualcomm chipsets, depending on the manufacturer and Android build used.

What does this mean?

Attackers can exploit the vulnerability through malicious applications or specially crafted requests that interact with the graphics driver**.**

Typical exploitation process:

1. **Triggering the calculation error**
    - A malicious app sends specially crafted input to the GPU driver.
    - The driver miscalculates the size of the memory buffer due to an integer overflow.
2. **Memory corruption occurs**
    - The system allocates insufficient memory for the data being processed.
    - The excess data **overflows into adjacent memory areas**.
3. **Privilege escalation**
    - Attackers may leverage the corrupted memory to **bypass Android security restrictions**.
4. **Potential attacker outcomes**
    - Gain **elevated system privileges**.
    - Execute arbitrary code on the device.
    - Access sensitive user data such as messages, camera, or files.

In targeted attacks, such exploits are often combined with spyware or other privilege-escalation exploits to fully compromise mobile devices.

Mitigation process

CERTVU recommend:

1. Apply Security Updates Immediately
2. Update Device Firmware

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://nvd.nist.gov/vuln/detail/CVE-2026-21385
3. https://www.cve.org/CVERecord?id=CVE-2026-21385