Annexure

NCA-21.01326 – National CERT Advisory – Android Zero-Day Exploit

1. INTRODUCTION

Based on the Android Security Bulletin for December 2025, Google has identified and addressed 107 distinct vulnerabilities, among which are 3 high-severity zero-day flaws that have been actively exploited in targeted attacks, specifically impacting devices running Android 13 and later. These critical vulnerabilities within the Android Framework merit immediate action across the public sector, considering the extensive usage of Android phones by employees. The gist of mitigation measures includes installing the latest Android Security Updates at the earliest, enabling and keeping Google Play Protect active, and downloading verified apps from the Google Play Store only while avoiding the installation of untrusted third-party apps using APKs.

2. VULNERABILITIES & IMPACT

a. **CVE-2025-48633 - Info Disclosure.** It allows attackers to access sensitive data leveraging leak memory contents and bypassing protections. Vulnerability is actively exploited in real-world campaigns, potentially tied to surveillance or spyware operations.

b. **CVE-2025-48572 - Elevation of Privilege.** It enables an attacker to gain higher permissions than intended, after gaining initial access to the sys.

c. **CVE-2025-48631.** A critical remote Denial of Svc (DoS) flaw in the framework that doesn't require executive privileges to trigger. Affected versions include Android 13, 14, 15, and 16.

3. AFFECTED DEVICES & ROLLOUT STATUS

Devices remain at risk until the security patch is installed. As per December 2025, devices updates are as under:

a. **Google Pixel Devices.** December 2025 security updates are available and should be installed immediately.

b. **Samsung & Other OEMs.** Patch rollout may lag; some devices may not receive updates until late Jan 2026 or even later.
c. **Enterprise Devices.** Devices under enterprise mgmt may receive patches based on firm's IT policy.
d. **Unpatched Devices.** Remain susceptible until updated.

4. RECOMMENDED MITIGATIONS

The December 2025 Android security update is critical due to active exploitation of the vulnerabilities as under:

a. Immediate Actions (All Users)

(1) Install the latest December 2025 Android Security Update as soon as it appears on your device.

(2) Confirm your Security Patch Lvl is 2025-12-05 or later.

(3) Avoid installation of unverified apps from third-party app sources until updates are applied.

b. Enterprise & Managed Android Phones

(1) Enforce compulsory update policies via MDM (Mobile Device Management).

(2) Monitor devices for signs of compromise (crash logs, privilege abuse).

(3) Restrict access from unpatched devices to sensitive system.

c. Additional Best Practices

(1) Enable Google Play Protect and keep it active.

(2) Back up critical data regularly.

(3) Educate users on phishing and tgt attk indicators.

5. CALL TO ACTION

To protect systems and information, all personnel using Android devices for work **must immediately** complete the following critical actions:

1. Install the December 2025 security update.
2. Enable google play protect.
3. Use official app sources only.
4. Ensure widespread awareness and conduct spot checks and awareness drives where possible.

The time to act is ***now***! Delaying these steps leaves devices and entire networks exposed to active threats. Please confirm compliance to IT or security point of contact.