NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT-021-99213409
Karachi, Dated: 27th January, 2026

To

1. The Chairman, Planning & Development Board Sindh, Karachi
2. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
3. The Chairman/Chairperson, CMIT Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh_____.
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). _____.
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh_____.

SUBJECT: CYBERSECURITY ADVISORY ON ANDROID ZERO-DAY EXPLOIT-IMMEDIATE ACTION REQUIRED

In view of the recently disclosed and actively exploited Android zero-day vulnerabilities, the attached Advisory titled "National CERT Advisory - Android Zero-Day Exploit (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT), based on the Android Security Bulletin for December 2025.

2. The Advisory highlights the presence of multiple high-severity vulnerabilities, including zero-day flaws under active exploitation, affecting Android devices running version 13 and above. It outlines the associated risks, potential impact on information security, and prescribes urgent mitigation measures, including immediate installation of the December 2025 Android Security Update, enforcement of mobile device security controls, and adoption of recommended best practices to safeguard organizational and national digital assets.

3. It is requested, that attached Advisory may kindly be disseminated to all concerned departments, organizations, and personnel under your administrative control, particularly those using Android devices for official purposes. Necessary actions may be initiated on priority to ensure timely patching, heightened vigilance, and strict compliance with the recommended security measures.

Annexure: NCA-21.011326-National CERT Advisory - Android Zero-Day Exploit

(DR. RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II

A copy is forwarded for information and necessary action to: -

1. Chief Executive Officer Sindh IT Company (SITC), Karachi.
2. Director General (nCERT). L Block, Pak Secretariat, Islamabad
3. AS(Staff) to Chief Minister Sindh, Karachi.
4. Director (Operations), S&IT Department, Govt. of Sindh
5. PS to Chief Secretary, Sindh.
6. Staff Officer to Special Assistant to Chief Minister Sindh, S&IT Department, Govt. of Sindh, Karachi.
7. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
8. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.
9. Webmaster, for uploading the advisory on url: *https://www.sindh.gov.pk/*

NOTE: In case of further guidance please feel free to contact 0310-2131415

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 ment 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: