



GOVERNMENT OF PAKISTAN
MINISTRY OF FEDERAL EDUCATION AND PROFESSIONAL TRAINING



No.F. NO. 2(4)/2026-COORD

Islamabad, the 20th January , 2026

From

Ishtiaq Ahmad
Section Officer (Coord)

To

1- Executive Director, HEC, Islamabad

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

Please find enclosed herewith a copy of the National CERT Advisory, letter No. 1-1/2026/DG (NCERT)/ 67 dated 20th January 2026, on the subject cited above, which is self-explanatory, for information and further necessary action

Encl: (As above)

Irfan Ali
Assistant-I (Coordination)
20 January , 2026, 10:32:24 AM

**Ishtiaq Ahmad
Section Officer (Coord)**

Copy for information to:-

- 1- Additional Secretary, MOFEPT, Islamabad
- 2- Sr Joint Secretary (Admin/Coord), MOFEPT, Islamabad
- 3- Sr. Joint Secretary (HEC), MOFEPT, Islamabad
- 4- SJS FE/PT, MOFEPT, Islamabad
- 5- JS IC, MOFEPT, Islamabad
- 6- DS Council/Legal/Coord&Audit, MOFEPT, Islamabad
- 7- PSOtoSec, MOFEPT, Islamabad

**Ishtiaq Ahmad
Section Officer (Coord)**

Priority



GOVERNMENT OF PAKISTAN
NCERT



No.1-1/2026/DG (NCERT)/ 67

Islamabad, the 20th January , 2026

From

Dr Haider Abbas
DG -(nCERT)

To

- 1- Secretary NTISB, CAB, Islamabad
- 2- Secretary, MOPNR, Islamabad
- 3- Secretary Religious Affairs, MORA, Islamabad
- 4- Secretary, MONFSR, Islamabad
- 5- Chairman (SECP), SECP, Islamabad
- 6- Chairman OGRA, OGRA, Islamabad
- 7- Acting Chairman HEC, HEC, Islamabad
- 8- Chairman NEPRA, NEPRA, Islamabad
- 9- Director General, PCAA, Karachi
- 10- Secretary, Science and Technology Balochistan,
- 11- Chief Secretary KPK, Govt of Khyber Pakhtun Khawa,
- 12- Chief Secretary Sindh, Govt of Sindh,
- 13- Cheif Secretary AJK, Govt of Azad Jammu and Kashmir,
- 14- Chief Secretary Punjab, Govt of Punjab,
- 15- Chief Secretary GB, Govt of Gilgit Baltistan,
- 16- Chief Secretary Balochistan, Govt of Balochistan,
- 17- Secretary Information, Science and Technology Department Government of Sindh,
- 18- Secretary, Information Technology Department Gilgit Baltistan Government of Gilgit Baltistan,
- 19- Cabinet Secretary, CAB, Islamabad
- 20- Chief Secretary (GB), CSGB, Barmas Gilgit
- 21- Federal Secretary (MoCommunication), MOCM, Islamabad
- 22- Federal Secretary of MoNHS, MONHS, Islamabad
- 23- Foreign Secretary, MOFA, Islamabad
- 24- Secretary, REVDIV, Islamabad
- 25- Secretary, NSD, Islamabad
- 26- Secretary, MOD, Rawalpindi
- 27- Secretary, MOEPWD, Islamabad
- 28- Secretary, NHCD, Islamabad
- 29- Secretary, MOWR, Islamabad
- 30- Secretary, MOHR, Islamabad
- 31- Secretary, TEOR, Islamabad
- 32- Secretary, MOC, Islamabad
- 33- Secretary (DP), MODP, Rawalpindi
- 34- Secretary (EAD), EAD, Islamabad
- 35- Secretary (Education), MOFEPT, Islamabad

- 36- Secretary (Railways), MOR, Islamabad
- 37- Secretary Climate Change, MOCC, Islamabad
- 38- Secretary Establishment Division, ESTAB, Islamabad
- 39- Secretary FPSC, FPSC, Islamabad.
- 40- Secretary Finance, MOF, Islamabad
- 41- Secretary Housing, MOHW, Islamabad
- 42- Secretary IPC, MOIPC, Islamabad
- 43- Secretary IT, MoIT, Islamabad
- 44- Secretary Industries & Production, MOIP, Islamabad
- 45- Secretary Kashmir Affair, Gilgit Baltistan & SAFRON, kagbsafron, Islamabad
- 46- Secretary LAW & Justice, MOLJ, Islamabad
- 47- Secretary Maritime Affairs, MOMA, Islamabad
- 48- Secretary Ministry of Parliamentary Affairs, MOPA, Islamabad
- 49- Secretary MoIBC, MOIBC, Islamabad
- 50- Secretary Planning, PC, Islamabad
- 51- Secretary Privatisation Division, PRIDIV, Islamabad
- 52- Secretary SIFC, SIFC, Islamabad
- 53- Secretary Science and Technology, MOST, Islamabad
- 54- Secretary of Interior, MOINC, Islamabad
- 55- Secretary(MoPHRD), MOPHRD, Islamabad
- 56- Secretary, PA&SS Division, PASS, Islamabad

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 the 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 compliance with the recommended security measures.

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



Dr Haider Abbas
DG -(nCERT)
Ph:03009634911

Irfan Ali
Assistant-I (Coordination)
22 January , 2026, 10:30:02 AM



National Cyber Emergency Response Team

Government of Pakistan



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.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



- 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:

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



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.



National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk