NCA-28.231126– National CERT Advisory

Multiple Vulnerabilities in WhatsApp for Android, iOS, Windows and Mac Desktop

Background

WhatsApp has published its 2026 security advisories covering five vulnerabilities fixed in the May and November 2026 updates: **CVE-2026-102769**, **CVE-2026-44908**, **CVE-2026-23871**, **CVE-2026-23866** and **CVE-2026-23863**. They affect WhatsApp and WhatsApp Business on Android, iOS and Mac Desktop, and WhatsApp for Windows. The flaws could allow deletion of locally stored files, limited leakage of chat database information, disclosure of a device's IP address, processing of attacker controlled media or URLs on a victim's device, and execution of a malicious file disguised as a harmless document. Most require the user to open or interact with a crafted message or file. WhatsApp reports no evidence of in the wild exploitation for four of the five vulnerabilities; however, for CVE-2026-23871, it states the issue may have been abused together with specific spam messages.

Affected Products and Potential Risks

Users running WhatsApp versions earlier than the fixed releases below are affected:

- **CVE-2026-102769** – WhatsApp for Android before 2.26.35.74. SQL injection via a crafted "order details" message from an unofficial client could delete local WhatsApp files and, if the user is online, leak one bit of chat database information through a crash and delivery receipt timing side channel.
- **CVE-2026-44908** – WhatsApp for iOS before 2.26.24.72; WhatsApp Business for iOS and WhatsApp for Mac Desktop before 2.26.23.72; WhatsApp for Android before 2.26.23.74; WhatsApp Business for Android before 2.26.23.70. Improper certificate chain validation in the Meta AI confidential-computing attestation verifier could let an attacker positioned within Meta infrastructure bypass the hardware root of trust. WhatsApp's transparency ledger shows no exploitation.
- **CVE-2026-23871** – WhatsApp and WhatsApp Business for Android before 2.26.17.4. Incomplete validation of ad reply URLs in a crafted Click to WhatsApp message could reveal the device's IP information to an attacker.
- **CVE-2026-23866** – WhatsApp for iOS 2.25.8.0 to 2.26.15.72 and Android 2.25.8.0 to 2.26.7.10. Incomplete validation of AI rich response messages could trigger processing of media from an

arbitrary URL, including OS custom URL scheme handlers (Fixed in iOS 2.26.15.73+ and Android 2.26.7.11+).

- **CVE-2026-23863** – WhatsApp for Windows before 2.3000.1032164386.258709. A filename with embedded NUL bytes could make a malicious executable appear as another file type and run when opened.

Recommendations

National CERT advises all government institutions, public and private organizations and individual users of WhatsApp to implement the following measures on priority:

S. No.	Recommended Measures	Actions Required
1	**Update WhatsApp Immediately**	Update WhatsApp and WhatsApp Business on all platforms to the latest version from the official app store or the vendor's website, at or above the fixed versions listed above.
2	**Identify Installed Versions**	Inventory WhatsApp installations on managed Android, iOS, Windows and Mac devices, verify versions and prioritize users handling sensitive information.
3	**Use Official Clients Only**	Do not install unofficial or modified WhatsApp clients or sideloaded builds, which are a source of crafted malicious messages.
4	**Treat Unexpected Messages with Caution**	Do not tap unexpected "order details" or ad reply messages, or Click to WhatsApp ads from unknown senders. Avoid opening documents from unverified senders and check the actual file type before opening on Windows.
5	**Enforce Update Controls**	Enable automatic updates and use device management policies to block outdated WhatsApp versions on organizational devices where feasible.
6	**Strengthen Endpoint Protection**	Keep endpoint security active on Windows and Mac systems so that executables disguised as documents are detected and blocked.
7	**Report and Respond**	Block and report suspicious accounts and messages in the app. Report suspected compromise to your security team and to National CERT.

8	**Disable Media Auto-Download**	As a defense-in-depth measure for stronger protection against future attacks alongside updating WhatsApp, users and administrators should disable automatic downloading of media and documents Configure WhatsApp settings (and MDM/device policies where applicable) to disable automatic downloading of media and documents (set media auto-download to Never / off across mobile data and Wi-Fi) to reduce exposure to malicious files. **Android:** Go to Settings → Storage and data → Media auto-download, open When using mobile data, When connected on Wi-Fi, and When roaming, and uncheck Photos, Audio, Videos, and Documents in all three options. **iPhone (iOS):** Go to Settings → Storage and Data → Media Auto-Download, and set Photos, Audio, Video, and Documents to Never.

REFERENCE

WhatsApp Security Advisories, 2026 Updates (May and November 2026):
https://www.whatsapp.com/security/advisories

For other advisories, please visit the National CERT website: https://pkcert.gov.pk/advisories

National Cyber Emergency Response Team (National CERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad
+92-51-9203422
info@pkcert.gov.pk
www.pkcert.gov.pk