WhatsApp has a serious security vulnerability, which Google has publicly disclosed.

Google Project Zero has revealed a serious security vulnerability in WhatsApp for Android that allows malicious files to be downloaded without user interaction. What can users do to protect themselves?

WhatsApp is currently the world's largest online messaging platform, boasting a rich ecosystem of features, an ad-free interface, and widespread use not only for personal but also professional purposes in many organizations. However, this very popularity also makes WhatsApp an attractive target for security attacks. Recently, the Google Project Zero team publicly disclosed a critical vulnerability in WhatsApp for Android, after Meta failed to fully fix it within the standard 90-day deadline.

According to Brendon Tiszka, a member of the Project Zero team, the attacker simply creates a WhatsApp group, then adds the victim and an acquaintance of the victim to the group. Next, the attacker makes that acquaintance the group administrator and sends a malicious multimedia file. Due to WhatsApp's default settings, this file is automatically downloaded to the victim's device without any action from them. The media file is then saved to the Android MediaStore database, and if it manages to escape this sandbox environment, it becomes an exploit that allows for completely non-interaction attacks on the user.

While this vulnerability sounds alarming, it still has some limiting conditions. First, the attacker must know or guess the victim's phone number as well as the phone numbers of their acquaintances, which isn't too difficult in today's context but still presents a significant hurdle. Additionally, the malicious multimedia file needs to be sophisticated enough to execute harmful actions after being downloaded. Notably, if users enable the Advanced

Chat Privacy feature on WhatsApp or disable automatic media downloads, malicious files will not be downloaded automatically, significantly reducing the risk.

Google Project Zero stated that they privately reported the vulnerability to Meta on September 1, 2025, and gave the company 90 days to address it before making it public. However, as of November 30, 2025, Meta had still not released a complete patch, forcing Google to publicly disclose the vulnerability. On December 4, Tiszka confirmed that Meta had implemented a partial server-side fix, but a comprehensive solution was still under development. Since then, the ticket has not received any further updates, suggesting that the vulnerability likely remains unresolved.

According to Google Project Zero, this vulnerability **only affects WhatsApp on Android** . Users of iOS and other platforms are currently considered safe.

To reduce risk, Android users should:

1. **To enable Advanced chat privacy** in WhatsApp groups:
   Go to the group ? tap the three dots ? *Group info* ? turn on *Advanced chat privacy* .
2. **Turn off automatic media downloads** :
   Go to *Settings* ? *Storage and data* ? *Media auto-download* .

Notably, Meta admitted to a vulnerability related to WhatsApp attachments last year, suggesting that this continues to be an attractive attack surface for malicious actors in recent times.