New zero-click exploit allegedly used to hack WhatsApp users

Data: 2025-08-29 22:43:47

Autor: Inteligência Against Invaders

New zero-click exploit allegedly used to hack WhatsApp users

WhatsApp warns users targeted by advanced spyware, sending threat notifications to affected individuals from the past 90 days.

A new zero-click exploit used to hack WhatsApp users, reported Donncha Ó Cearbhaill, Head of Security Lab at @AmnestyTech.

WhatsApp has just sent out a round of threat notifications to individuals they believe were targeted by an advanced spyware campaign in the past 90 days. WhatsApp warns some users that a malicious message may have exploited OS flaws to compromise devices and data. Donncha Ó Cearbhaill is seeking out expert help after receiving this alert. The attack requires no user interaction, meaning victims could be compromised without clicking a link or downloading a file. Such exploits are typically linked to well-resourced threat actors, including state-sponsored groups. WhatsApp urges recipients of the notification to review their devices for unusual behavior, update to the latest version, and enable enhanced security measures to reduce the risk of further compromise.

WhatsApp announced that it had already patched the flaw exploited by attackers, but risks remain.

> ? BREAKING: New zero-click exploit used to hack WhatsApp users.
>
> WhatsApp has just sent out a round of threat notifications to individuals they believe where targeted by an advanced spyware campaign in past 90 days.
>
> Seek out expert help if you have received this alert pic.twitter.com/i4cHLsiNOr
>
> — Donncha Ó Cearbhaill (@DonnchaC) August 29, 2025

Below is the text sent to the impacted users:

“Our investigation indicates that a malicious message may have been sent to you through WhatsApp and combined with other vulnerabilities in your device’s operating system to compromise your device and the data it contains, including messages.

While we don’t know with certainty that your device has been compromised, we wanted to let you know out of an abundance of caution so you can take steps to secure your device and information.

We’ve made changes to prevent this specific attack from occurring through WhatsApp. However, your device’s operating system could remain compromised by the malware or be targeted in other ways.

To best protect yourself, we recommend a full device factory reset. We also strongly urge you to keep your devices updated to the latest version of the operating system, and ensure that your WhatsApp app is up to date.”

Commercial spyware vendors are behind most zero-day exploits discovered by researchers in the wild. Zero-day exploits are essential components is stealth spyware campaigns.

Surveillance software is used to spy on high-risk users, including journalists, human rights defenders, dissidents and opposition party politicians.

The surveillance industry is experiencing exponential growth, fueled by the sustained demand from rogue governments, intelligence agencies, and malicious actors for sophisticated malware and surveillance tools.

In early August, Meta **announced** it is sponsoring ZDI’s Pwn2Own Ireland 2025 hacking competition, where participants can earn big prizes for smartphone, WhatsApp and wearable device exploits. Participants can earn up to $1 million for a WhatsApp exploit that allows attackers to achieve remote code execution with no user interaction.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,WhatsApp)