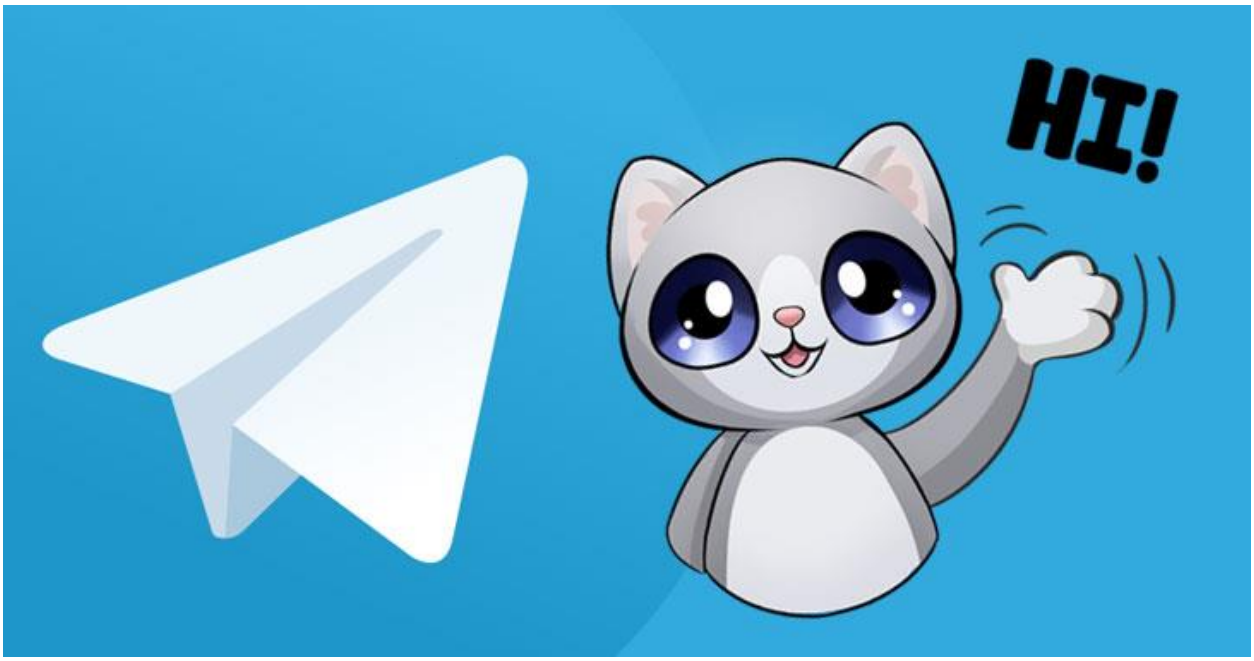
A Sticker Sent on Telegram Could Have Exposed Your Secret Chats



Cybersecurity researchers on Monday disclosed details of a now-patched flaw in the Telegram messaging app that could have exposed users' secret messages, photos, and videos to remote malicious actors.

The issues were discovered by Italy-based Shielder in iOS, Android, and macOS versions of the app. Following responsible disclosure, Telegram addressed them in a series of patches on September 30 and October 2, 2020.

The flaws stemmed from the way secret chat functionality operates and in the app's handling of animated stickers, thus allowing attackers to send malformed stickers to unsuspecting users and gain access to messages, photos, and videos that were exchanged with their Telegram contacts through both classic and secret chats.

One caveat of note is that exploiting the flaws in the wild may not have been trivial, as it requires chaining the aforementioned weaknesses to at least one additional vulnerability in order to get around security defenses in modern devices today. That might sound prohibitive, but, on the contrary, they are well in the reach of both cybercrime gangs and nation-state groups alike.

Shielder said it chose to wait for at least 90 days before publicly revealing the bugs so as to give users ample time to update their devices.

"Periodic security reviews are crucial in software development, especially with the introduction of new features, such as the animated stickers," the researchers said. "The

flaws we have reported could have been used in an attack to gain access to the devices of political opponents, journalists or dissidents."

It's worth noting that this is the second flaw uncovered in Telegram's secret chat feature, following last week's reports of a privacy-defeating bug in its macOS app that made it possible to access self-destructing audio and video messages long after they disappeared from secret chats.

This is not the first-time images, and multimedia files sent via messaging services have been weaponized to carry out nefarious attacks.

In March 2017, researchers from Check Point Research revealed a new form of attack against web versions of Telegram and WhatsApp, which involved sending users seemingly innocuous image files containing malicious code that, when opened, could have allowed an adversary to take over users' accounts on any browser completely, and access victims' personal and group conversations, photos, videos, and contact lists.

Recommendations:

- Don’t download version 7.1.0 in android, version 7.1 in iOS and macOS or older;
- Always check for latest updates on your devices;
- Run antivirus in your devices;
- And always cleanup your devices.

References :

- https://thehackernews.com/2021/02/a-sticker-sent-on-telegram-could-have.html?&web_view=true
- https://www.somagnews.com/telegram-your-secret-chats-revealed-by-a-sticker/
- https://securityaffairs.co/wordpress/114653/hacking/telegram-flaw-access-secret-chats.html