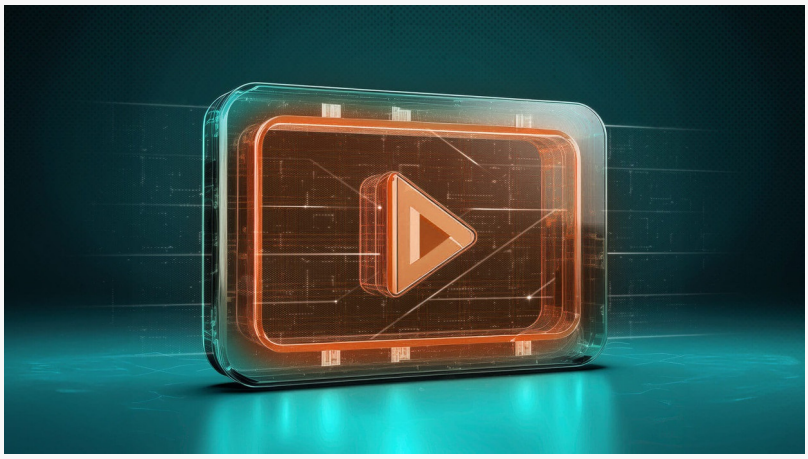
ESET Research discovers EvilVideo: Telegram app for Android targeted by zero-day exploit sending malicious videos



DUBAI, DUBAI, UNITED ARAB EMIRATES, July 22, 2024 /EINPresswire.com/ -- ESET researchers discovered a zero-day exploit, which targets the Telegram app for Android, that appeared for sale for an unspecified price in an underground forum post from June 2024.

Using the exploit to abuse a vulnerability that ESET named "EvilVideo," attackers could share malicious Android payloads via Telegram channels, groups, and chats, and make them appear to be multimedia files.

"We found the exploit being advertised for sale on an underground forum. In the post, the seller shows screenshots and a video of testing the exploit in a public Telegram channel. We were able to identify the channel in question, with the exploit still available. That allowed us to get our hands on the payload and test it ourselves," explains ESET researcher Lukáš Štefanko, who discovered the Telegram exploit.

ESET Research analysis of the exploit revealed that it works on Telegram versions 10.14.4 and older. The reason might be that the specific payload is most likely crafted using the Telegram API, since it allows developers to upload specially crafted multimedia files to Telegram chats or channels programmatically.

The exploit seems to rely on the threat actor being able to create a payload that displays an Android app as a multimedia preview and not as a binary attachment. Once shared in chat, the malicious payload appears as a 30-second video.

By default, media files received via Telegram are set to download automatically. This means that users with this option enabled will automatically download the malicious payload once they open the conversation where it was shared.

The default automatic download option can be disabled manually — in that case, the payload can still be downloaded by tapping the download button of the shared video.

If the user tries to play the “video,” Telegram displays a message that it is unable to play the video and suggests using an external player. However, if the user taps the Open button in the displayed message, they will be requested to install a malicious app disguised as the aforementioned external app.

After discovering the EvilVideo vulnerability on June 26, 2024, ESET followed coordinated disclosure policy and reported it to Telegram, but received no response at the time. We reported the vulnerability again on July 4, and that time, Telegram reached out to ESET the same day to confirm that its team was investigating EvilVideo. Telegam then fixed the issue, shipping version 10.14.5 on July 11. The vulnerability affected all versions of Telegram for Android up to 10.14.4, but has been updated as of version 10.14.5.

For more information about EvilVideo, read the blogpost “Cursed tapes: Exploiting the EvilVideo vulnerability in Telegram for Android” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET

ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — securing businesses, critical infrastructure, and individuals. Whether it’s endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. An ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

---

in today's world. Please see our Editorial Guidelines for more information.