Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

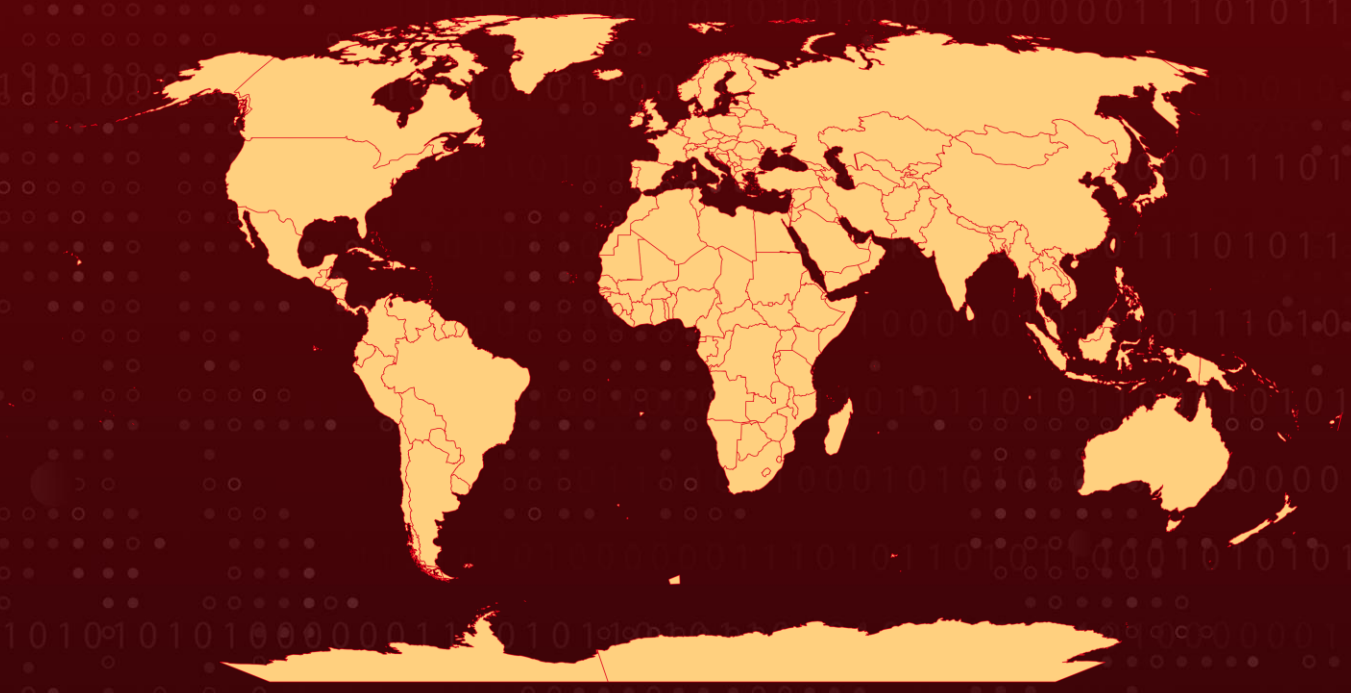
30-Second Video of Doom: EvilVideo Zero-Day Hits Telegram

Date of Publication	Admiralty Code	TA Number
July 24, 2024	A1	TA2024281

Summary

Attack Commenced: June 2024
Affected Product: Telegram
Targeted Region: Worldwide
Attack: In June 2024, a zero-day vulnerability known as 'EvilVideo' was discovered, allowing attackers to send malicious Android APK payloads disguised as video files. This vulnerability targeted the Telegram app for Android and was advertised for sale on the Russian-speaking XSS hacking forum by a seller named 'Ancryno.'

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
Unassigned	EvilVideo Vulnerability	Telegram Android versions 10.14.4 and older	✓	✗	✓

Attack Details

#1 A zero-day vulnerability dubbed 'EvilVideo' enabled attackers to send malicious Android APK payloads disguised as video files. This flaw specifically targeted the Telegram app for Android and was offered for sale at an unspecified price on an underground forum in June 2024.

#2 The seller, known by the moniker ‘Ancryno,’ advertised the exploit on the Russian-speaking XSS hacking forum. Threat actors had a grey window of at least five weeks to exploit this Telegram zero-day before it was patched on July 11, 2024.

#3 The exploit is effective only on Android Telegram versions 10.14.4 and older. It is speculated that the payload was crafted using the Telegram API, which allows for the programmatic upload of specially crafted multimedia files to Telegram chats or channels. The EvilVideo vulnerability enabled attackers to create malicious APK files that appeared as embedded 30-second videos when sent to other users on Telegram.

#4 By default, the Telegram app on Android automatically downloads media files, meaning channel participants receive the payload once they open the conversation. When victims attempt to play the fake video, Telegram prompts them to use an external player, potentially leading them to tap the "Open" button and execute the payload.

#5 Subsequently, victims must enable the installation of unknown apps from the device settings to allow the malicious APK file to be installed on their devices. Additionally, the seller shared another dubious service. Apart from the EvilVideo exploit, they have been promoting an Android cryptor-as-a-service on the same underground forum, claiming it to be fully undetectable (FUD).

Recommendations

Immediate Software Updates: Ensure to update the Telegram app to the latest version (post-July 11, 2024) to mitigate the EvilVideo vulnerability. Regularly check for updates and patches for all applications to stay protected against newly discovered vulnerabilities.

Enhanced Media Handling: Disable automatic media downloads in messaging apps to prevent malicious files from being downloaded without user consent. Advise users to avoid opening unsolicited video files or media from unknown sources.

User Education and Awareness: Educate users about the risks of zero-day vulnerabilities and the importance of cautious behavior when receiving files and links. Promote awareness of the steps needed to enable the installation of unknown apps, highlighting the associated risks.

Access Control Mechanisms: Implement strict access control mechanisms to limit permissions and reduce the risk of unauthorized access. Use multi-factor authentication (MFA) to add an extra layer of security to user accounts and sensitive systems.

Mobile Device Management (MDM): Implement MDM solutions to manage and secure mobile devices accessing corporate resources. Enforce security policies, such as device encryption and remote wipe capabilities, to protect sensitive data on mobile devices.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**T1036.004** Masquerade Task or Service
T1664 Exploitation for Initial Access	**T1658** Exploitation for Client Execution	**T1569** System Services	**T1569.002** Service Execution
T1566.001 Spearphishing Attachment	**T1204.002** Malicious File	**T1623** Command and Scripting Interpreter	**T1036** Masquerading

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	f159886dcf9021f41eaa2b0641a758c4f0c4033d

TYPE	VALUE
File Name	Teating.apk
IPv4	183[.]83[.]172[.]232
Domain	infinityhackscharan[.]ddns[.]net

Patch Details

Telegram for Android has been patched in version 10.14.5 and later.

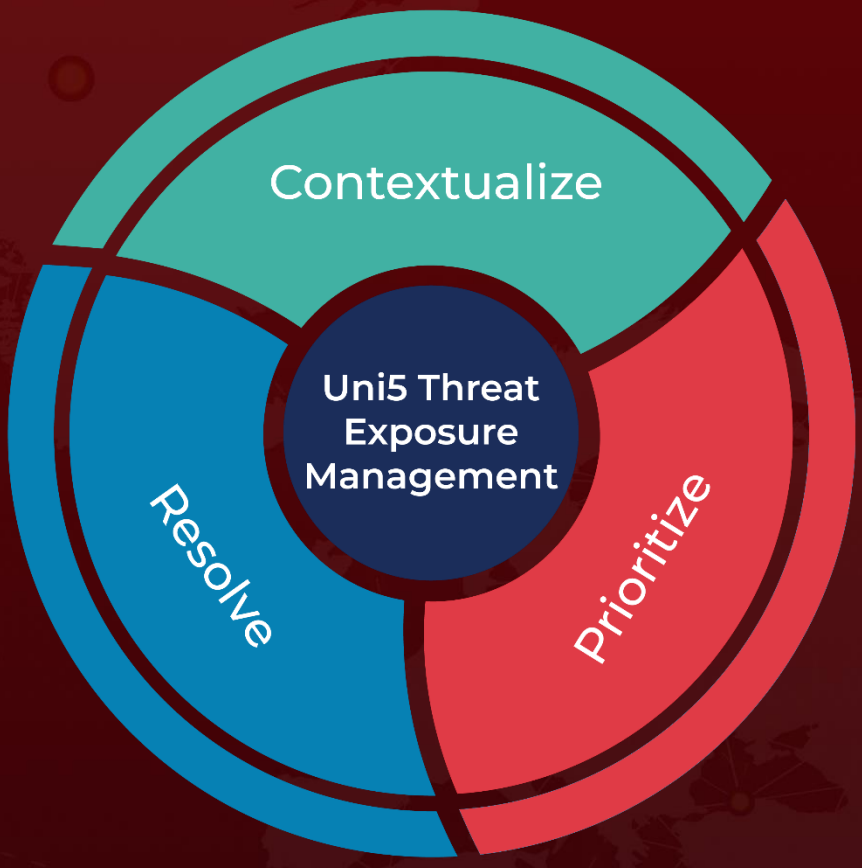
References

https://www.welivesecurity.com/en/eset-research/cursed-tapes-exploiting-evilvideo-vulnerability-telegram-android/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 24, 2024 • 5:00 AM

More at www.hivepro.com