The malicious video file causes users to lose control of the device 'storming' in the Android world

During this time, you should be more careful before accessing or playing any new strange videos that appear on your smartphone, especially videos downloaded from the Internet or received via strange email.

Are you, or your friends, relatives using Android devices?

If yes, please pay attention! During this time, you should be more careful before accessing or playing any new strange videos that appear on your smartphone, especially videos downloaded from the Internet or received via strange email.

Recently, network security experts from several reputable security groups have discovered an unusual appearance of a strange video file, which looks relatively harmless, but can have terrible consequences. against the victim's system.

1. Your computer can be hacked after opening a document in LibreOffice

The vulnerability allows hackers to execute code remotely on the victim's Android device

Specifically, this video file was designed to specifically target the destruction of your Android smartphone through a dangerous remote code execution vulnerability, which could allow hackers to execute custom code. comments on the victim's system. According to an unofficial statistics, this new but extremely effective attack has affected more than 1 billion devices running the Android operating system worldwide, the most popular of which is devices running on Android versions from 7.0 to 9.0 (Nougat, Oreo or Pie).

This remote code execution vulnerability is currently being tracked under the name CVE-2019-2107, appearing in the Android media framework. CVE-2019-2107, rated at a high risk level because if successfully exploited, this vulnerability could allow the remote attacker to execute arbitrary code on the targeted device that the user does not well know before they can make a response.

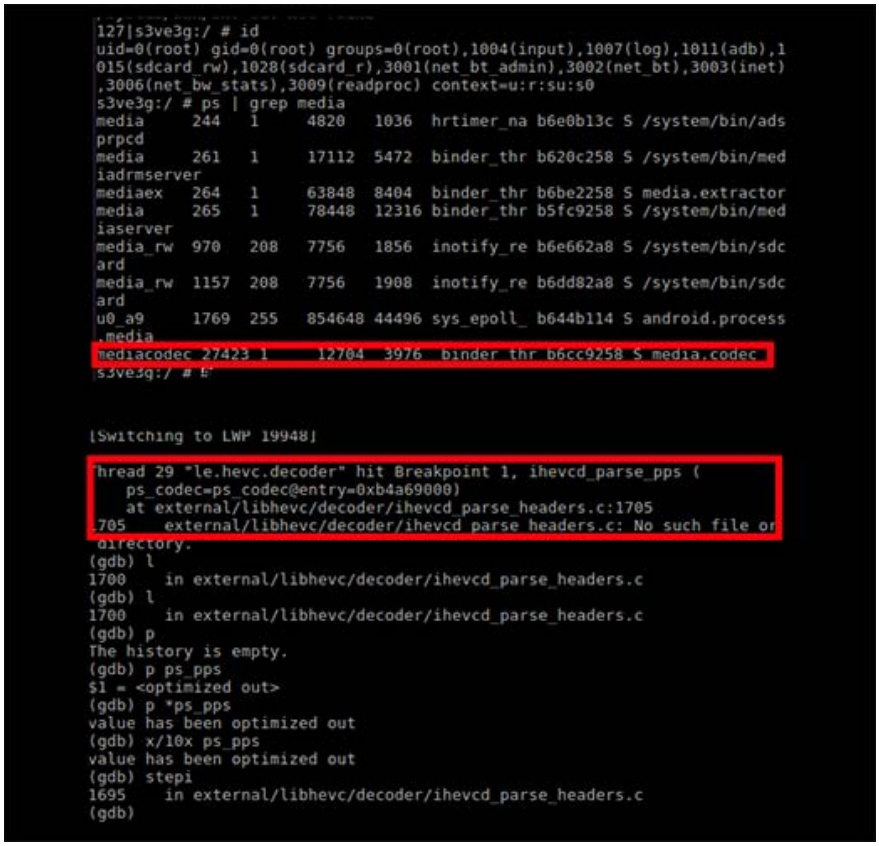
1. Agent Smith code is threatening 25 million Android devices

To take full control of the target device, all the attacker needs to do is trick the user into opening a malicious video file sent to the device. This video file is also specially created with the original Android video player application.

Although Google has released a small security patch earlier this month to address the vulnerability, it is clear that millions of Android devices still cannot access the latest security update, which needs to be provided by each vendor of the device, which makes light or unknown users information about this vulnerability continue to risk becoming its victim. Google briefly described this vulnerability in the July security newsletter as follows:

"This critical vulnerability is related to Android's media framework, so it can allow remote attackers to use specially crafted files to execute arbitrary code in the context of a privileged process" .

1. Even if denied access, thousands of Android applications can still track you



This serious vulnerability is related to Android's media framework

In a related move, the famous Android application developer Marcin Kozlowski recently published proof-of-concept (PoC) on a typical strike based on CVE-2019-2107 on Github , raising concerns about if Android device

manufacturers will not soon send security patches to users, the number of victims of this vulnerability will increase significantly in the near future.

In Marcin Kozlowski's PoC, the malicious file used is a HEVC encoded video. Not only does it ruin the media player, it can also help potential attackers develop new exploits to achieve the ultimate goal of completely controlling the victim's device.

However, it should be noted that if these malicious videos are sent to and received via several instant messaging applications such as WhatsApp, Facebook Messenger or uploaded to a video streaming service such as YouTube or Twitter . hackers will not be able to launch the attack. This is because the above services often compress videos and re-encode the entire media file, thereby causing the malicious code embedded in the video to be "deformed" completely, unable to work.

1. Many Android users discover that their phones have spyware installed after traveling to China

Avoid downloading and playing random video files from unreliable sources

In short, until you get additional security patches from the publisher, the best way to avoid becoming a victim and protecting yourself from this attack is to avoid downloading and playing random video files. of course from unreliable sources, along with complying with all basic privacy and privacy guidelines.

Finally, don't forget to update your mobile operating system as soon as the latest patch arrives!

You finished reading the article "**The malicious video file causes users to lose control of the device 'storming' in the Android world**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.