

Forum:[Hack Forums](#)

Thread: [Android Stagefright vulnerability is Back - 10 Sec to Hack Android Device](#)

Ov3rFI0w - March 17, 2016, 4:16 pm

Attention Android users!

Millions of Android devices are vulnerable to hackers and intelligence agencies once again – Thanks to a newly disclosed Android Stagefright Exploit.

Yes, Android Stagefright vulnerability is Back...

...and this time, the Stagefright exploit allows an attacker to hack Android smartphones in 10 seconds just by tricking users into visiting a hacker's web page that contains a malicious multimedia file. A group of security researchers from Israel-based research firm NorthBit claimed it had successfully exploited the Stagefright bug that was emerged in Android last year and described as the "worst ever discovered". The new Stagefright exploit, dubbed Metaphor, is detailed in a research paper [PDF] that guides bad guy, good guy as well as government spying agencies to build the Stagefright exploit for themselves.

Just yesterday, we reported about critical vulnerabilities in Qualcomm Snapdragon chip that could be exploited by any malicious application to gain root access on a vulnerable Android device, leaving more than a Billion Android devices at risk.

Video Demonstration — Exploit to Hack Android Phone in 10 Seconds

The researchers have also provided a proof-of-concept video demonstration that shows how they successfully hacked an Android Nexus 5 device using their Metaphor exploit in just 10 seconds. They also successfully tested Metaphor on a Samsung Galaxy S5, LG G3 and HTC One smartphones.

[Video: <https://www.youtube.com/watch?v=I507kD0zG6k>]

According to the researchers, Millions of unpatched Android devices are vulnerable to their exploit that successfully bypasses security defenses offered by Android operating system.

What is StageFright Bug and Why You have to Worry about it

Stagefright is a multimedia playback library, written in C++, built inside the Android operating system to process, record and play multimedia files such as videos.

However, what Zimperium researchers discovered last year was that this core Android component can be remotely exploited to hijack 95 percent of Android devices with just a simple booby-trapped message or web page. Another critical vulnerability discovered last October in Stagefright exploited flaws in MP3 and MP4 files, which when opened were capable of remotely executing malicious code on Android devices, and was dubbed Stagefright 2.0. However, to tackle this serious issue, Google released a security update that patches the critical bug as well as promised regular security updates for Android smartphones following the seriousness of the Stagefright bugs.

Here's How the New Stagefright Exploit Works

Researchers described the following process to successfully hijack any vulnerable Android smartphone or tablet:

Step 1: Tricking a victim into visiting a malicious web page containing a video file that crashes the Android's mediaserver software to reset its internal state.

Step 2: Once the mediaserver gets a restart, JavaScript on the web page sends information about the victim's device over the Internet to the attacker's server.

Step 3: The attacker's server then sends a custom generated video file to the affected device, exploiting the Stagefright bug to reveal more info about the device's internal state.

Step 4: This information is also sent back to the attacker's server to craft another video file that embeds a payload of malware in it, which when processed by Stagefright starts executing on the victim's smartphone with all the privileges it needs to spy on its owner.

The researchers also claim that their exploit specifically attacks the CVE-2015-3864 vulnerability in a way that bypasses Address Space Layout Randomisation (ASLR), a memory protection process.

[\(Source\)](#)

Abathur - March 17, 2016, 5:04 pm

This is a quality post, thank you for sharing!

TeddyMedina - May 3, 2017, 3:06 pm

I've found no tool or exploit for this vulnerability.

Any help ?

occupi - May 3, 2017, 3:06 pm

This post is over a year old, that's probably why.

TeddyMedina - May 3, 2017, 3:57 pm

(May 3, 2017 03:07 PM)Yani Wrote: [\[CITE\]](#) This is from a year ago.

What are you looking for?

Thanks Yani,

A tool that use this vulnerability.