Haktuts

All About Ethical Hacking,Hacking News,Security News,Privacy Issue,Cyber Crime,Pentesting Tools,Open Sources,Cyber Security,How-To,Tips And Tricks And Dark Web News

# Google patches critical media processing and rooting vulnerabilities in Android

## The flaws can be exploited remotely through emails, Web pages, MMS and rogue apps

Google has released a new batch of security fixes for its Nexus smartphones and tablets, addressing flaws that could allow attackers to compromise the Android devices via rogue emails, Web pages, and MMS messages.

Firmware updates are being rolled out to supported Nexus devices as an over-the-air update and the patches will be added the Android Open Source Project (AOSP) over the next 48 hours. Builds LMY48Z and Android Marshmallow with a Dec. 1, 2015, Security Patch Level contain these fixes, Google said in its security bulletin.

The updates address five vulnerabilities rated as critical, 12 rated as high and two as moderate. A significant number of flaws were again located in the OS' media processing components, which handle audio and video file playback and corresponding file metadata parsing.

One of the critical vulnerabilities is located in mediaserver, a core part of the operating system, and can be exploited to execute arbitrary code with privileges that third-party applications are not supposed to have. Attackers can exploit the flaw remotely by tricking users into playing specifically crafted media files in their browsers or by sending them via multimedia message (MMS).

It's worth noting that Google has disabled automatic parsing of multimedia messages received in Google Hangouts and Messenger, the default messaging applications in Android.

Three other media processing vulnerabilities that can lead to remote code execution via email, Web browsing and MMS have been patched in the Skia graphics engine and the user mode display driver loaded by mediaserver.

The last critical vulnerability patched in this release is a privilege escalation flaw in the Android kernel. It potentially allows rogue applications to execute code as root, the highest privilege on the system.

This is the type of flaw that enables so-called Android rooting, which some enthusiasts use to gain complete control over their devices. But in the hands of malicious attackers, such a flaw can lead to a full and persistent device compromise that can only be fixed by re-flashing the operating system.

Additional privilege escalation flaws have been fixed in other components with this release, but they're rated only as high because they don't provide root access. They can, however, give rogue apps dangerous permissions that they shouldn't have.

Google recommends that users of older Android versions update to the latest one, if possible -- for example, if their device manufacturers provided updates. That's because newer versions of Android have security enhancements in place that can make exploitation of some vulnerabilities harder or impossible.

Google's security team also uses features like Verify Apps and SafetyNet to monitor for and block potentially harmful applications. For example, apps that use privilege escalation flaws to root devices are not allowed in Google Play and Verify Apps will block known rooting apps by default.

## Also See:

1. Critical Vulnerabilities Discovered in 3G/4G Modems Includes "Remote Code Execution,Cross-Site Request Forgery And Cross-Site Scripting"
2. 6.1 Million smart devices at risk from 3 year old flaw
3. Anonymous Accuses "Cloudflare" For Protecting ISIS Sites
4. Snowden Unveils NSA "God Mode" Malware That Lives On Your Motherboard And Can Not Be Traced
5. Here's How Google Can "Remotely Bypass" Pattern Lock Of Android Device
6. Nmap7:The New Version Of Nmap Released After 3.5 Years