Google patched Nexus devices, including a critical Wi-Fi flaw

February 7, 2016 By Pierluigi Paganini

Google announced to have patched a number of critical vulnerabilities affecting the Nexus devices that lead to the complete hack of the device.

Google announced to have patched a critical vulnerability affecting the Nexus devices that could be exploited by an attacker on the same Wi-Fi network. The company confirmed that it is not aware of attacks in the wild exploiting the vulnerabilities.

The patch issued by Google fixes several vulnerabilities in the Broadcom Wi-Fi driver that could be exploited by an attacker for remote code execution. The updates are available in the builds LMY49G or later for Nexus devices, the fix has been distributed on Jan. 4 through carrier and manufacturer partners. The same updates will be very soon available for the Android Open Source Project.

sending a malicious wireless control message packet that could corrupt kernel memory and lead the remote code execution at the kernel level.

“Multiple remote execution vulnerabilities in the Broadcom Wi-Fi driver could allow a remote attacker to use specially crafted wireless control message packets to corrupt kernel memory in a way that leads to remote code execution in the context of the kernel. These vulnerabilities can be triggered when the attacker and the victim are associated with the same network. This issue is rated as a Critical severity due to the possibility of remote code execution in the context of the kernel without requiring user interaction.” states the Nexus Security Bulletin – February 2016.

The vulnerabilities coded as CVE-2016-0801 and CVE-2016-0802, were privately reported to Google by the Broadgate Team on October 25.

Google has also issued a fix for a new problem in the Mediaserver that could be exploited in several ways, for example by sending an MMS file.

“During media file and data processing of a specially crafted file, vulnerabilities in mediaserver *could allow an attacker to cause memory corruption and remote code execution as the* mediaserver *process.*

The affected functionality is provided as a core part of the operating system and there are multiple applications that allow it to be reached with remote content, most notably MMS and browser playback of media.” continues the Advisory.

“This issue is rated as a Critical severity due to the

possibility of remote code execution within the context of the mediaserver *service. The* mediaserver *service has access to audio and video streams as well as access to privileges that third-party apps cannot normally access."*

Google fixed also a critical vulnerability, coded as CVE-2016-0807, affecting the Debuggerd component that could be exploited by hackers to root the Android device.

The Google bulletin also patches two other critical vulnerabilities in Qualcomm modules (CVE-2016-0805 and CVE-2016-0806) the Qualcomm Performance Module and the Qualcomm Wi-Fi Driver. The flaws allow the elevation of privilege for an attacker. In the case of the Qualcomm performance event manager component for ARM processors an attacker can exploit it by using a local application to run code at the kernel level.

In the case of the Qualcomm Wi-Fi driver, the attacker can use a local application to run code at the kernel level as well.

Pierluigi Paganini

(Security Affairs – Android Google Nexus, Wi-Fi)

Android | Google Nexus | Hacking | mobile | Wi-Fi

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
The UN panel rules Julian Assange is in arbitrary detention

NEXT ARTICLE
How to thwart the passcode lock screen on iOS 8 and 9?

YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6 Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

The IPT ruled that GCHQ spies can legally hack any electronic devices

February 13, 2016 By Pierluigi Paganini

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group,

he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top