Nexus Security Bulletin - March 2016

Published March 07, 2016 | Updated March 08, 2016

We have released a security update to Nexus devices through an over-the-air (OTA) update as part of our Android Security Bulletin Monthly Release process. The Nexus firmware images have also been released to the Google Developer site (https://developers.google.com/android/nexus/images). Builds LMY49H or later and Android M with Security Patch Level of March 01, 2016 or later address these issues. Refer to the Nexus documentation (https://support.google.com/nexus/answer/4457705) for instructions on how to check the security patch level.

Partners were notified about the issues described in the bulletin on February 1, 2016 or earlier. Where applicable, source code patches for these issues have been released to the Android Open Source Project (AOSP) repository.

The most severe of these issues is a Critical security vulnerability that could enable remote code execution on an affected device through multiple methods such as email, web browsing, and MMS when processing media files. The severity assessment (https://source.android.com/security/overview/updates-resources.html#severity) is based on the effect that exploiting the vulnerability would possibly have on an affected device, assuming the platform and service mitigations are disabled for development purposes or if successfully bypassed.

We have had no reports of active customer exploitation of these newly reported issues. Refer to the Mitigations (#mitigations) section for details on the Android security platform protections (https://source.android.com/security/enhancements/index.html) and service protections such as SafetyNet, which improve the security of the Android platform. We encourage all customers to accept these updates to their devices.

Mitigations

This is a summary of the mitigations provided by the Android security platform (https://source.android.com/security/enhancements/index.html) and service protections such as SafetyNet. These capabilities reduce the likelihood that security vulnerabilities could be successfully exploited on Android.

- Exploitation for many issues on Android is made more difficult by enhancements in newer versions of the Android platform. We encourage all users to update to the latest version of Android where possible.
- The Android Security team is actively monitoring for abuse with Verify Apps and SafetyNet which will warn about potentially harmful applications about to be installed. Device rooting tools are prohibited within Google Play. To protect users who install applications from outside of Google Play, Verify Apps is enabled by default and will warn users about known rooting applications. Verify Apps attempts to identify and block installation of known malicious applications that exploit a privilege escalation vulnerability. If such an application has already been installed, Verify Apps will notify the user and attempt to remove any such applications.
- As appropriate, Google Hangouts and Messenger applications do not automatically pass media to processes such as mediaserver.

Acknowledgements

We would like to thank these researchers for their contributions:

- Abhishek Arya, Oliver Chang, and Martin Barbella of Google Chrome Security Team: CVE-2016-0815
- Anestis Bechtsoudis (@anestisb (https://twitter.com/anestisb)) of CENSUS S.A.: CVE-2016-0816, CVE-2016-0824
- Chad Brubaker from Android Security: CVE-2016-0818
- Mark Brand of Google Project Zero: CVE-2016-0820
- Mingjian Zhou (@Mingjian_Zhou (https://twitter.com/Mingjian_Zhou)), Chiachih Wu (@chiachih_wu (https://twitter.com/chiachih_wu)), and Xuxian Jiang of C0RE Team (http://c0reteam.org) from Qihoo 360 (http://www.360safe.com): CVE-2016-0826
- Peter Pi (@heisecode (https://twitter.com/heisecode)) of Trend Micro: CVE-2016-0827, CVE-2016-0828, CVE-2016-0829
- Scott Bauer (sbauer@eng.utah.edu (mailto:sbauer@eng.utah.edu), sbauer@plzdonthack.me (mailto:sbauer@plzdonthack.me)): CVE-2016-0822
- Wish Wu (@wish_wu (https://twitter.com/@wish_wu)) of Trend Micro Inc.: CVE-2016-0819
- Yongzheng Wu and Tieyan Li of Huawei: CVE-2016-0831
- Su Mon Kywe and Yingjiu Li of Singapore Management University: CVE-2016-0831

- Zach Riggle (@ebeip90 (https://twitter.com/@ebeip90)) of the Android Security Team: CVE-2016-0821

Security Vulnerability Details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2016-03-01 patch level. There is a description of the issue, a severity rationale, and a table with the CVE, associated bug, severity, affected versions, and date reported. When available, we will link the AOSP change that addressed the issue to the bug ID. When multiple changes relate to a single bug, additional AOSP references are linked to numbers following the bug ID.

Remote Code Execution Vulnerability in Mediaserver

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.

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 could not normally access.

CVE Bugs with AOSP links

CVE-2016-0815	ANDROID-26365349 (https://android.googlesource.com/platform%2Fframeworks%2Fav/+/5403587a74aee2fb57076528c3927851531c8afb)	
CVE-2016-0816	ANDROID-25928803 (https://android.googlesource.com/platform/external/libavc/+/4a524d3a8ae9aa20c36430008e6b	

Remote Code Execution Vulnerabilities in libvpx

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.

The issues are rated as Critical severity because they could be used for 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.

CVE Bug with AOSP links

CVE-2016-1621	ANDROID-23452792 (https://android.googlesource.com/platform/frameworks/av/+/5a6788730acfc6fd8f4a6ef89d2c3 [2] (https://android.googlesource.com/platform/external/libvpx/+/04839626ed859623901ebd3a5fd4 [3] (https://android.googlesource.com/platform/external/libvpx/+/5a9753fca56f0eeb9f61e342b2f

Elevation of Privilege in Conscrypt

A vulnerability in Conscrypt could allow a specific type of invalid certificate, issued by an intermediate Certificate Authority (CA), to be incorrectly trusted. This may enable a man-in-the-middle attack. This issue is rated as a Critical severity due to the possibility of an elevation of privilege and remote arbitrary code execution.

CVE Bug with AOSP links

CVE-2016-0818	ANDROID-26232830 (https://android.googlesource.com/platform/external/conscrypt/+/c4ab1b959280413fb11bf4fd7f [2] (https://android.googlesource.com/platform/external/conscrypt/+/4c9f9c2201116acf790fca25af

Elevation of Privilege Vulnerability in the Qualcomm Performance Component

An elevation of privilege vulnerability in the Qualcomm performance component could enable a local malicious application to execute arbitrary code in the kernel. This issue is rated as a Critical severity due to the possibility of a local permanent device compromise, and the device could only be repaired by re-flashing the operating system.

CVE	Bug	Severity	Updated versions	Date reported
CVE-2016-0819	ANDROID-25364034*	Critical	4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1	Oct 29, 2015

* The patch for this issue is not in AOSP. The update is contained in the latest binary drivers for Nexus devices available from the Google Developer site (https://developers.google.com/android/nexus/drivers).

Elevation of Privilege Vulnerability in MediaTek Wi-Fi Kernel Driver

There is a vulnerability in the MediaTek Wi-Fi kernel driver that could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as a Critical severity due to the possibility of elevation of privilege and arbitrary code execution in the context of the kernel.

CVE	Bug	Severity	Updated versions	Date reported
CVE-2016-0820	ANDROID-26267358*	Critical	6.0.1	Dec 18, 2015

* The patch for this issue is not in AOSP. The update is contained in the latest binary drivers for Nexus devices available from the Google Developer site (https://developers.google.com/android/nexus/drivers).

Elevation of Privilege Vulnerability in Kernel Keyring Component

An elevation of privilege vulnerability in the Kernel Keyring Component could enable a local malicious application to execute arbitrary code within the kernel. This issue is rated as a Critical severity due to the possibility of a local permanent device compromise and the device could potentially only be repaired by re-flashing the operating system. However, in Android versions 5.0 and above, SELinux rules prevents third-party applications from reaching the affected code.

Note: For reference, the patch in AOSP is available for specific kernel versions: 4.1 (https://android.googlesource.com/kernel/common/+/8a8431507f8f5910db5ac85b72dbdc4ed8f6b308), 3.18 (https://android.googlesource.com/kernel/common/+/ba8bb5774ca7b1acc314c98638cf678ce0beb19a), 3.14 (https://android.googlesource.com/kernel/common/+/93faf7ad3d603c33b33e49318e81cf00f3a24a73), and 3.10 (https://android.googlesource.com/kernel/common/+/9fc5f368bb89b65b591c4f800dfbcc7432e49de5).

CVE	Bug	Severity	Updated versions	Date reported
CVE-2016-0728	ANDROID-26636379	Critical	4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1	Jan 11, 2016

Mitigation Bypass Vulnerability in the Kernel

A mitigation bypass vulnerability in the kernel could permit a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. This issue is rated as High severity because it could permit a bypass of security measures in place to increase the difficulty of attackers exploiting the platform.

Note: The update for this issue is located in the Linux upstream (https://github.com/torvalds/linux/commit/8a5e5e02fc83aaf67053ab53b359af08c6c49aaf).

CVE	Bug	Severity	Updated versions	Date reported
CVE-2016-0821	ANDROID-26186802	High	6.0.1	Google Internal

Elevation of Privilege in MediaTek Connectivity Kernel Driver

There is an elevation of privilege vulnerability in a MediaTek connectivity kernel driver that could enable a local malicious application to execute arbitrary code within the context of the kernel. Normally a kernel code execution bug like this would be rated critical, but because it requires first compromising the conn_launcher service, it justifies a downgrade to High severity rating.

CVE	Bug	Severity	Updated versions	Date reported

CVE-2016-0822	ANDROID-25873324*	High	6.0.1	Nov 24, 2015

* The patch for this issue is not in AOSP. The update is contained in the latest binary drivers for Nexus devices available from the Google Developer site (https://developers.google.com/android/nexus/drivers).

Information Disclosure Vulnerability in Kernel

An information disclosure vulnerability in the kernel could permit a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. These issues are rated as High severity because they could allow a local bypass of exploit mitigation technologies such as ASLR in a privileged process.

Note: The fix for this issue is located in Linux upstream (https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ab676b7d6fbf4b294bf198fb27ade5b0e865c7ce)

.

CVE	Bug	Severity	Updated versions	Date reported
CVE-2016-0823	ANDROID-25739721*	High	6.0.1	Google Internal

* The patch for this issue is not in AOSP. The update is contained in the latest binary drivers for Nexus devices available from the Google Developer site (https://developers.google.com/android/nexus/drivers).

Information Disclosure Vulnerability in libstagefright

An information disclosure vulnerability in libstagefright could permit a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. These issues are rated as High severity because they could also be used to gain elevated capabilities, such as Signature (http://developer.android.com/guide/topics/manifest/permission-element.html#plevel) or SignatureOrSystem (http://developer.android.com/guide/topics/manifest/permission-element.html#plevel) permissions privileges, which are not accessible to third-party applications.

CVE	Bug with AOSP link

CVE-2016-0824	ANDROID-25765591 (https://android.googlesource.com/platform/external/libmpeg2/+/ffab15eb80630dc799eb41085

Information Disclosure Vulnerability in Widevine

An information disclosure vulnerability in the Widevine Trusted Application could allow code running in the kernel context to access information in TrustZone secure storage. This issue is rated as High severity because it could be used to gain elevated capabilities, such as Signature (http://developer.android.com/guide/topics/manifest/permission-element.html#plevel) or SignatureOrSystem (http://developer.android.com/guide/topics/manifest/permission-element.html#plevel) permissions privileges.

CVE	Bug(s)	Severity	Updated versions	Date reported
CVE-2016-0825	ANDROID-20860039*	High	6.0.1	Google Internal

* The patch for this issue is not in AOSP. The update is contained in the latest binary drivers for Nexus devices available from the Google Developer site (https://developers.google.com/android/nexus/drivers).

Elevation of Privilege Vulnerability in Mediaserver

An elevation of privilege vulnerability in mediaserver could enable a local malicious application to execute arbitrary code within the context of an elevated system application. This issue is rated as High severity because it could be used to gain elevated capabilities, such as Signature (http://developer.android.com/guide/topics/manifest/permission-element.html#plevel) or SignatureOrSystem (http://developer.android.com/guide/topics/manifest/permission-element.html#plevel) permissions privileges, which are not accessible to a third-party application.

CVE	Bugs with AOSP links
CVE-2016-0826	ANDROID-26265403 (https://android.googlesource.com/platform/frameworks/av/+/c9ab2b0bb05a7e19fb057e79b3 [2] (https://android.googlesource.com/platform/frameworks/av/+/899823966e78552bb6dfd7772

CVE-2016-0827	ANDROID-26347509 (https://android.googlesource.com/platform/frameworks/av/+/9e29523b9537983b4c4b205ff8680827)

Information Disclosure Vulnerability in Mediaserver

An information disclosure vulnerability in mediaserver could permit a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. These issues are rated as High severity because they could also be used to gain elevated capabilities, such as Signature (http://developer.android.com/guide/topics/manifest/permission-element.html#plevel) or SignatureOrSystem (http://developer.android.com/guide/topics/manifest/permission-element.html#plevel) permissions privileges, which are not accessible to third-party applications.

CVE Bugs with AOSP links

CVE-2016-0828	ANDROID-26338113 (https://android.googlesource.com/platform/frameworks/native/+/dded8fdbb700d6cc498debc690828)
CVE-2016-0829	ANDROID-26338109 (https://android.googlesource.com/platform/frameworks/native/+/d06421fd37fbb7fd07002e6738)

Remote Denial of Service Vulnerability in Bluetooth

A remote denial of service vulnerability in the Bluetooth component could allow a proximal attacker to block access to an affected device. An attacker could cause an overflow of identified Bluetooth devices in the Bluetooth component, which leads to memory corruption and service stop. This is rated as a High severity because it leads to a Denial of Service to the Bluetooth service, which could potentially only be fixed with a flash of the device.

CVE Bug with AOSP link

	ANDROID-26071376

CVE-
2016-
0830

Information Disclosure Vulnerability in Telephony

An information disclosure vulnerability in the Telephony component could allow an application to access sensitive information. This issue is rated Moderate severity because it could be used to improperly access data without permission.

CVE	Bug with AOSP link
CVE-2016-0831	ANDROID-25778215 (https://android.googlesource.com/platform/frameworks/opt/telephony/+/79eecef63f3ea996883

Elevation of Privilege Vulnerability in Setup Wizard

A vulnerability in the Setup Wizard could enable an attacker who had physical access to the device to gain access to device settings and perform a manual device reset. This issue is rated as Moderate severity because it could be used to improperly work around the factory reset protection.

CVE	Bug(s)	Severity	Updated versions	Date reported
CVE-2016-0832	ANDROID-25955042*	Moderate	5.1.1, 6.0, 6.0.1	Google Internal

* There is no source code patch provided for this update.

Common Questions and Answers

This section reviews answers to common questions that may occur after reading this bulletin.

1. How do I determine if my device is updated to address these issues?

Builds LMY49H or later and Android 6.0 with Security Patch Level of March 1, 2016 or later address these issues. Refer to the Nexus documentation

(https://support.google.com/nexus/answer/4457705) for instructions on how to check the security patch level. Device manufacturers that include these updates should set the patch string level to: [ro.build.version.security_patch]:[2016-03-01]

Revisions

- March 07, 2016: Bulletin published.
- March 08, 2016: Bulletin revised to include AOSP links.