# CERT-MU Advisory

CERT-MU

**CERT-MU AD-2016-06**

## MULTIPLE VULNERABILITIES IN ANDROID DEVICES

**Original Issue Date:** 08 September 2016

**Severity Rating:** High

**Overview:**

Multiple vulnerabilities have been identified in Android devices. These vulnerabilities could be exploited by attackers to gain elevated privileges, cause execution of arbitrary code, disclose user information and cause denial of service condition on the target system. Android has issued updates to addresses these vulnerabilities.

**Description:**

Multiple vulnerabilities have been identified in Android devices. These vulnerabilities could be exploited by attackers to gain elevated privileges, cause remote code execution, disclose user information and cause denial of service condition on the target system.

The vulnerabilities reported are as follows:

- A vulnerability has been identified in LibUtils. This vulnerability could enable an attacker using a specially crafted file to execute arbitrary code in the context of a privileged process. Successful exploitation of this vulnerability could allow an attacker to cause remote code execution.

- A vulnerability has been identified in Mediaserver. This vulnerability could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. Successful exploitation of this vulnerability could allow an attacker to cause remote code execution.

- A vulnerability has been identified in MediaMuxer. This vulnerability could allow an attacker using a specially crafted file to execute arbitrary code in the context

of an unprivileged process. Successful exploitation of this vulnerability could allow an attacker to cause remote code execution.

- A vulnerability has been identified in Mediaserver. This vulnerability could allow a local malicious application to execute arbitrary code within the context of a privileged process. Successful exploitation of this vulnerability could allow an attacker to gain elevated privileges.

- A vulnerability has been identified in Mediaserver. This vulnerability could allow an attacker to use a specially crafted file to cause a device hang or reboot. Successful exploitation of this vulnerability could cause a denial of service condition.

- A vulnerability has been identified in the Telephony component. This vulnerability could allow a local malicious application to send unauthorized premium SMS messages. Successful exploitation of this vulnerability could allow an attacker to gain elevated privileges.

- A vulnerability has been identified in the integrated Android debugger. This vulnerability could allow a local malicious application to execute arbitrary code. Successful exploitation of this vulnerability could allow an attacker to gain elevated privileges.

- A vulnerability has been identified in Settings. This vulnerability could allow a local malicious application to bypass operating system protections for VPN settings.

- A vulnerability has been identified in SMS. This vulnerability could allow a local attacker to send premium SMS messages prior to the device being provisioned.

- A vulnerability has been identified in Java Debug Wire Protocol. This vulnerability could allow a local malicious application to cause execution of arbitrary code.

- A vulnerability has been identified in AOSP Mail. This vulnerability could allow a local malicious application to gain access to user's private information.

- A vulnerability has been identified in the kernel security subsystem. This vulnerability could allow a local malicious application to cause execution of arbitrary code.

- A vulnerability has been identified in the kernel USB driver. This vulnerability could allow a local malicious application to cause execution of arbitrary code.
- A vulnerability has been identified in the Qualcomm radio interface layer. This vulnerability could allow a local malicious application to cause execution of arbitrary code.
- A vulnerability has been identified in the Synaptics touchscreen driver. This vulnerability could allow a local malicious application to execute arbitrary code.
- A vulnerability has been identified in the Broadcom Wi-Fi driver. This vulnerability could allow a specially crafted application to cause execution of arbitrary code.
- A vulnerability has been identified in the kernel shared memory subsystem. This vulnerability could allow a specially crafted application to cause execution of arbitrary code.
- A vulnerability has been identified in the Qualcomm networking component. This vulnerability could allow a local malicious application to execute arbitrary code.

**Impact of the attack(s)**

An attacker can:

- cause remote code execution,
- gain elevated privileges,
- cause denial of service,
- cause disclosure of user information.

**Affected System:**

- Android AOSP prior to versions 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0
- Nexus 5, Nexus 6, Nexus 9, Nexus Player, Android One ,Nexus 5X, Nexus 6P, Pixel C, Android One

**CVE Information:**

CVE-2016-3861
CVE-2016-3862
CVE-2016-3863
CVE-2016-3875
CVE-2016-3883
CVE-2016-3884
CVE-2016-3888

More CVE information available on: https://source.android.com/security/bulletin/2016-09-01.html#2016-09-01-summary

**Solution**

Users are advised to apply updates.

- **2016-09-01**: Partial security patch level string. This security patch level string indicates that all issues associated with 2016-09-01 (and all previous security patch level strings) are addressed.
- **2016-09-05**: Partial security patch level string. This security patch level string indicates that all issues associated with 2016-09-01 and 2016-09-05 (and all previous security patch level strings) are addressed.
- **2016-09-06**: Complete security patch level string, which addresses issues that were discovered after partners were notified of most issues in this bulletin. This security patch level string indicates that all issues associated with 2016-09-01, 2016-09-05, and 2016-09-06 (and all previous security patch level strings) are addressed.
- Supported Nexus devices will receive a single Over-The-Air (OTA) update with the 2016-09-06 security patch level.

More information about the updates is available on:
https://source.android.com/security/bulletin/2016-09-01.html#2016-09-01-summary

**References:**
**Android Security Bulletin**
https://source.android.com/security/bulletin/2016-09-01.html#2016-09-01-summary

**Disclaimer**
The information provided herein is on "as is" basis, without warranty of any kind. Please note that the members who do not want to receive the security alert, can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

**Hotline No:** (+230) 800 2378
**Fax No:** (+230) 208 0119
**Gen. Info**. : contact@cert.ncb.mu
**Incident:** incident@cert.ncb.mu
**Website:** http://cert-mu.org.mu