



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

September 7, 2016

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2016-129

DATE(S) ISSUED:

09/07/2016

SUBJECT:

Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices including, but not limited to smartphones, tablets, and watches. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, information disclosure, or bypassing security restrictions.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Android OS builds prior to versions 6.1, 7.0 and Security Patch Levels earlier than September 06, 2016.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Google's Android OS is prone to multiple vulnerabilities, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Remote code execution vulnerability in LibUtils with the use of a specially crafted file (CVE-2016-3861).
- Remote code execution vulnerability in Mediaserver with the use of a specially crafted file (CVE-2016-3862).
- Remote code execution vulnerability in MediaMuxer with the use of a specially crafted file (CVE-2016-3863).
- Elevation of privilege vulnerability in Mediaserver Could allow for a local malicious application to execute arbitrary code (CVE-2016-3870, CVE-2016-3871, CVE-2016-3872).
- Elevation of privilege during the boot sequence could allow a local malicious attacker to boot into sage mode even though it's disabled (CVE-2016-3875).
- Elevation of privilege in Settings could enable a local malicious attacker to boot into safe mode (CVE-2016-3876).
- Denial of service vulnerability in Mediaserver with the use of a specially crafted file (CVE-2016-3899, CVE-2016-3878, CVE-2016-3879, CVE-2016-3880, CVE-2016-3881).
- Elevation of privilege vulnerability in the Telephony component allows a local malicious application to send unauthorized premium SMS messages (CVE-2016-3883).
- Elevation of privilege vulnerability in the Notification Manager Service allows a local malicious application to bypass operating system protections that isolate applications data (CVE-2016-3884).
- Elevation of privilege vulnerability in the integrated Android debugger Allows a local malicious application to execute arbitrary code (CVE-2016-3885).
- Elevation of privilege in the System UI Tuner Allows a local malicious user to modify protected settings when the device is locked (CVE-2016-3886).
- Elevation of privilege vulnerability in Settings allows a local malicious application to bypass operating system protections for VPN settings (CVE-2016-3887).
- Elevation of privilege vulnerability in SMS allows a local attacker to send premium SMS messages prior to the device being provisioned (CVE-2016-3888).
- Elevation of privilege vulnerability in Settings allows a local attacker to bypass the Factory Reset Protection and gain access to the device (CVE-2016-3889).
- Elevation of privilege vulnerability in the Java Debug Wire Protocol allows a local malicious application to execute arbitrary code (CVE-2016-3890).
- Information disclosure vulnerability in Mediaserver allows a local malicious application to access data outside of its permissions level (CVE-2016-3895).
- Information disclosure vulnerability in AOSP Mail enables a local malicious application to gain access to the user's private information (CVE-2016-3896).
- Information disclosure vulnerability in the Wi-Fi configuration allows an application to access sensitive information (CVE-2016-3897).
- Denial of service vulnerability in the Telephony component enables a local malicious application to prevent 911 TTY calls from a locked screen (CVE-2016-3898).

- Elevation of privilege vulnerability in the kernel security subsystem enables a local malicious application to execute arbitrary code (CVE-2014-9529, CVE-2016-4470).
- Elevation of privilege vulnerability in the kernel networking subsystem enables a local malicious application to execute arbitrary code (CVE-2013-7446).
- Elevation of privilege vulnerability in the kernel netfilter subsystem enables a local malicious application to execute arbitrary code (CVE-2016-3134).
- Elevation of privilege vulnerability in the kernel USB driver enables a local malicious application to execute arbitrary code (CVE-2106-3951).
- Elevation of privilege vulnerability in the kernel sound subsystem allows for a local malicious application to execute arbitrary code (CVE-2014- 4655).
- Elevation of privilege vulnerability in the kernel ASN.1 decoder enables a local malicious application to execute arbitrary code (CVE-2016-2053).
- Elevation of privilege vulnerability in the Qualcomm radio interface layer enables a local malicious application to execute arbitrary code (CVE 2016-3864).
- Elevation of privilege vulnerability in the Qualcomm subsystem driver enables a local malicious application to execute arbitrary code (CVE-2106-3858).
- Elevation of privilege vulnerability in the kernel networking driver enables a local malicious application to execute arbitrary code (CVE-2016-4805).
- Elevation of privilege vulnerability in the Synaptics touchscreen driver enables a local malicious application to execute arbitrary code (CVE-2016-3865).
- Elevation of privilege vulnerability in the Qualcomm camera driver enables a local malicious application to execute arbitrary code(CVE-2016-3859).
- Elevation of privilege vulnerability in the Qualcomm sound driver enables a local malicious application to execute arbitrary code (CVE-2016-3866).
- Elevation of privilege vulnerability in the Qualcomm IPA driver enables a local malicious application to execute arbitrary code (CVE-2016-3867).
- Elevation of privilege vulnerability in the Qualcomm power driver enables a local malicious application to execute arbitrary code (CVE-2016-3868).
- Elevation of privilege vulnerability in the Broadcom Wi-Fi driver enables a local malicious application to execute arbitrary code (CVE-2016-3869).
- Elevation of privilege vulnerability in the kernel eCryptfs filesystem enables a local malicious application to execute arbitrary code (CVE-2016-1583).
- Elevation of privilege vulnerability in the NVIDIA kernel enables a local malicious application to execute arbitrary code (CVE-2016-3873).
- Elevation of privilege vulnerability in the Qualcomm Wi-Fi driver enables a local malicious application to execute arbitrary code (CVE-2016-3874).
- Denial of service vulnerability in the kernel networking subsystem enables an attacker to cause a device to hang or reboot (CVE-2015-1465, CVE-2015-5364).
- Denial of service vulnerability in the kernel ext4 file system allows an attacker to cause a local permanent denial of service (CVE-2015-8839).
- Information disclosure vulnerability in the Qualcomm SPMI driver enables a local malicious application to access data outside of its permission level (CVE-2106-3892).
- Information disclosure vulnerability in the Qualcomm sound codec enables a local malicious application to access data outside of its permission level (CVE-2016-3893).

- Information disclosure vulnerability in the Qualcomm DMA component enables a local malicious application to access data outside of its permission level (CVE-2016-3894).
- Information disclosure vulnerability in the kernel networking subsystem enables a local malicious application to access data outside of its permission level (CVE-2016-4998).
- Denial of service vulnerability in the kernel networking subsystem enables an attacker to block access to Wi-Fi capabilities (CVE-2015-2992).
- Elevation of privilege vulnerability in the kernel shared memory subsystem enables a local malicious application to execute arbitrary code (CVE-2016-5340).
- Elevation of privilege vulnerability in the Qualcomm networking component enables a local malicious application to execute arbitrary code (CVE-2016-2059).
- Multiple vulnerabilities exist in affecting Qualcomm components, including bootloader, camera driver, character driver, networking, sound driver, and video driver (CVE-2016-2469).

Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, information disclosure, or bypassing security restrictions.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Remind users to download apps only from trusted vendors in the Play Store.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Google:

<https://source.android.com/security/bulletin/2016-09-01.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-7446>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-4655>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9529>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-1465>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-2922>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-5364>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-8839>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-1583>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-2053>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-2059>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-2469>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-3134>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-3858>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-3859>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-3861>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-3862>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-3863>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-3864>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-3865>

