

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

01/05/2016

SUBJECT:

Multiple Vulnerabilities in Google Android Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Android, 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, phones, tablets, and watches. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment.

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

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

Android versions 6.0 and prior

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:

- Mediaserver is vulnerable to memory corruption and remote code execution when processing a specially crafted media or data file (CVE-2015-6636).
- An elevation of privilege vulnerability in the misc-sd driver from MediaTek could enable a local malicious application to execute arbitrary code within the kernel (CVE-2015-6637).

- An elevation of privilege vulnerability in a kernel driver from Imagination Technologies could enable a local malicious application to execute arbitrary code within the kernel (CVE-2015-6638).
- Elevation of privilege vulnerabilities in the Widevine QSEE TrustZone application could enable a compromise, privileged application with access to QSEECOM to execute arbitrary code in the Trustzone context (CVE-2015-6639, CVE-2015-6647).
- An elevation of privilege vulnerability in the kernel could enable a local malicious application to execute arbitrary code in the kernel (CVE-2015-6640).
- An elevation of privilege vulnerability in the Bluetooth component could enable a remote device paired over Bluetooth to gain access to user's private information (Contacts) (CVE-2015-6641).
- 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 (CVE-2015-6642).
- An elevation of privilege vulnerability in the Setup Wizard could enable an attacker with physical access to the device to gain access to device settings and perform a manual device reset (CVE-2015-6643).
- An elevation of privilege vulnerability in the Wi-Fi component could enable a locally proximate attacker to gain access to Wi-Fi service related information. (CVE-2015-5310).
- An information disclosure vulnerability in Bouncy Castle could enable a local malicious application to gain access to user's private information (CVE-2015-6644).
- A denial of service vulnerability in the SyncManager could enable a local malicious application to cause a reboot loop (CVE-2015-6645).
- SysV IPC is not supported in any Android Kernel. It has been removed from the OS as it exposes additional attack surface that doesn't add functionality to the system that could be exploited by malicious applications (CVE-2015-6646).

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

RECOMMENDATIONS:

The following actions should be taken:

- Android users should patch the device immediately after receiving the update notification from the device's carrier.
- Try contacting your device vendor to determine when a patch will be available, and to urge them to patch as soon as possible.
- If supported by your messaging apps, change the settings to prevent the device from automatically retrieving MMS messages and to block messages from unknown senders. If your app does not support either of these functionalities, consider switching to a messaging app that does.

REFERENCES:

Google:

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

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5310>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6636>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6637>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6638>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6639>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6640>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6641>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6642>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6643>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6644>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6645>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6646>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6647>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>