

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:

02/02/2016

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. Successful exploitation of these issues can allow an attacker to bypass security restrictions, perform unauthorized actions, obtain sensitive information, bypass same-origin policy restrictions to access data, and execute remote code in the context of the affected application.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- Android versions prior to 6.0

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:

- Multiple remote code execution vulnerabilities in the 'Broadcom Wi-Fi' driver when it processes specially crafted wireless control message packets. (CVE-2016-0801, CVE-2016-0802)
- Multiple remote code execution and memory corruption vulnerabilities in the 'Mediaserver' service when it processes a specially crafted file. (CVE-2016-0803, CVE-2016-0804)
- An elevation of privilege vulnerability in 'Qualcomm Performance Module' that could allow for a local malicious application to execute arbitrary code within the kernel. (CVE-2016-0805)

- An elevation of privilege vulnerability in 'Qualcomm Wifi Driver' that could allow for a local malicious application to execute arbitrary code within the context of the kernel. (CVE-2016-0806)
- An elevation of privilege vulnerability in the 'Debugged' component that could enable a local malicious application to execute arbitrary code within the device root context. (CVE-2016-0807)
- A denial of service vulnerability in the 'Minikin' library that could allow for a local attacker to temporarily block access to an affected device. (CVE-2016-0808)
- An elevation of privilege vulnerability in the Wi-Fi component that could enable a local malicious application to execute arbitrary code within the System context. (CVE-2016-0809)
- An elevation of privilege vulnerability in mediaserver that could enable a local malicious application to execute arbitrary code within the context of an elevated system application. (CVE-2016-0810)
- An information disclosure vulnerability in 'libmediaplayerservice' that could allow for a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. (CVE-2016-0811)
- An elevation of privilege of privilege vulnerability in 'Setup Wizard' that could allow for a malicious attacker to bypass the Factory Reset Protection and gain access to the device. (CVE-2016-0812, CVE-2016-0813)

Successful exploitation of these issues can allow an attacker to bypass security restrictions, perform unauthorized actions, obtain sensitive information, bypass same-origin policy restrictions to access data, and execute remote code in the context of the affected application.

RECOMMENDATIONS:

The following actions should be taken:

- Android users should patch the device immediately after receiving the update notification from your network carrier.
- Try contacting your network carrier to determine when a patch will be available, and to urge them to patch as soon as possible.
- Remind users to download apps only from trusted vendors in the Play Store.
- Run all software as a non-privileged/non-rooted user to diminish the effects of a successful attack.

REFERENCES:

Google:

<http://source.android.com/security/bulletin/2016-02-01.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0801>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0802>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0803>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0804>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0805>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0806>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0807>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0808>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0809>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0810>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0811>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0812>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0813>

TLP: WHITE

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

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