

*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:**

05/03/2016

**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 including 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, blocking access to a Bluetooth device, or bypassing security restrictions.

**THREAT INTELLIGENCE:**

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

**SYSTEM AFFECTED:**

Android OS builds prior to versions 6.0.1 and without Security Patch Levels of May 01, 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:

- Multiple remote code execution vulnerabilities exist in MediaServer. (CVE-2016-2428, CVE-2016-2429)
- An elevation of privilege vulnerability in Debuggerd. (CVE-2016-2430)
- Multiple elevation of privilege vulnerabilities in Qualcomm TrustZone. (CVE-2016-2431, CVE-2016-2432)

- Multiple elevation of privilege vulnerabilities in Qualcomm Wi-Fi Driver. (CVE-2015-0569, CVE-2015-0570)
- Multiple elevation of privilege vulnerabilities in NVIDIA Video Driver. (CVE-2016-2434, CVE-2016-2435, CVE-2016-2436, CVE-2016-2437)
- An elevation of privilege vulnerability in Kernel. (CVE-2015-1805)
- A remote code execution vulnerability exists in Kernel. (CVE-2016-2438)
- An information disclosure vulnerability exists in Qualcomm Tethering Controller. (CVE-2016-2060)
- A remote code execution vulnerability exists in Bluetooth. (CVE-2016-2439)
- An elevation of privilege vulnerability in Binder. (CVE-2016-2440)
- Multiple elevation of privilege vulnerabilities in Qualcomm Buspm Driver. (CVE-2016-2441, CVE-2016-2442)
- An elevation of privilege vulnerability in Qualcomm MDP Driver. (CVE-2016-2443)
- An elevation of privilege vulnerability in Qualcomm Wi-Fi Driver. (CVE-2015-0571)
- Multiple elevation of privilege vulnerabilities in NVIDIA Video Driver. (CVE-2016-2444, CVE-2016-2445, CVE-2016-2446)
- Multiple elevation of privilege vulnerabilities in Wi-Fi. (CVE-2016-2447, CVE-2016-2457)
- Multiple elevation of privilege vulnerabilities in Mediaserver. (CVE-2016-2448, CVE-2016-2449, CVE-2016-2450, CVE-2016-2451, CVE-2016-2452)
- Multiple elevation of privilege vulnerabilities in MediaTek Wi-Fi Driver. (CVE-2016-2453, CVE-2016-2456)
- A remote denial of service vulnerability in Qualcomm Hardware Codec. (CVE-2016-2454)
- Multiple elevation of privilege vulnerabilities in Conscript. (CVE-2016-2461, CVE-2016-2462)
- An elevation of privilege vulnerability in OpenSSL & BoringSSL. (CVE-2016-0705)
- An information disclosure vulnerability exists in AOSP Mail. (CVE-2016-2458)
- Multiple information disclosure vulnerabilities exist in MediaServer. (CVE-2016-2459, CVE-2016-2460)
- A denial of service vulnerability in Kernel. (CVE-2016-0774)

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

#### **RECOMMENDATIONS:**

The following actions should 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.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- 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/2016-05-01.html>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0569>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0570>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0571>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1805>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0705>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0774>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2060>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2428>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2429>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2430>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2431>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2432>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2434>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2435>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2436>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2437>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2438>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2439>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2440>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2441>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2442>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2443>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2444>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2445>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2446>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2447>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2448>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2449>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2450>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2451>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2452>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2453>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2454>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2456>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2457>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2458>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2459>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2460>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2461>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2462>

**TLP: WHITE**

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

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