

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:

06/07/2016

SUBJECT:

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

OVERVIEW:

Multiple vulnerabilities have been discovered in 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 currently 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 June 01, 2016 or later

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 Mediaserver with the use of a specially crafted file. (CVE-2016-2463)
- Remote code execution vulnerability in libwebm with the use of a specially crafted file. (CVE-2016-2464)

- Elevation of privilege vulnerability in the Qualcomm video driver with local application could lead to arbitrary code execution in a kernel context. (CVE-2016-2465, CVE-2016-2489)
- Elevation of privilege vulnerability in the Qualcomm sound driver with local application could lead to arbitrary code execution in a kernel context. (CVE-2016-2466, CVE-2016-2467, CVE-2016-2066, CVE-2016-2469)
- Elevation of privilege vulnerability in the Qualcomm GPU driver with local application could lead to arbitrary code execution in a kernel context. (CVE-2016-2468, CVE-2016-2062)
- Elevation of privilege vulnerability in the Qualcomm Wi-Fi driver with local application could lead to arbitrary code execution in a kernel context. (CVE-2016-2470, CVE-2016-2471, CVE-2016-2472, CVE-2016-2473, CVE-2016-2474)
- Elevation of privilege vulnerability in the Broadcom Wi-Fi driver with local application could lead to arbitrary code execution in a kernel context. (CVE-2016-2475, CVE-2016-2493)
- Elevation of privilege vulnerability in Mediaserver with local application could lead to arbitrary code execution in an elevated system application context. (CVE-2016-2476, CVE-2016-2477, CVE-2016-2478, CVE-2016-2479, CVE-2016-2480, CVE-2016-2481, CVE-2016-2482, CVE-2016-2483, CVE-2016-2484, CVE-2016-2485, CVE-2016-2486, CVE-2016-2487)
- Elevation of privilege vulnerability in the NVIDIA camera driver with local application could lead to arbitrary code execution in a kernel context. (CVE-2016-2490, CVE-2016-2491)
- Elevation of privilege vulnerability in the Qualcomm camera driver with local application could lead to arbitrary code execution in a kernel context. (CVE-2016-2061, CVE-2016-2488)
- Elevation of privilege vulnerability in the MediaTek Power Management driver with local application could lead to arbitrary code execution in a kernel context. (CVE-2016-2492)
- Elevation of privilege vulnerability in SD Card Emulation layer with local application could lead to arbitrary code execution in an elevated system application context. (CVE-2016-2494)
- Remote denial of service vulnerability in Mediaserver with the use of a specially crafted file. (CVE-2016-2495)
- Elevation of privilege vulnerability in the Framework UI could lead to unauthorized access to private files. (CVE-2016-2496)
- Information disclosure vulnerability in the Qualcomm Wi-Fi driver. (CVE-2016-2498)
- Information disclosure vulnerability in Mediaserver. (CVE-2016-2499)
- Information disclosure vulnerability in Activity Manager. (CVE-2016-2500)

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:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2492>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2493>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2494>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2495>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2496>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2498>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2499>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2500>

TLP: WHITE

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

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