

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:

12/30/2015

SUBJECT:

Multiple Vulnerabilities in Google Android Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Android 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 could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, or bypassing security restrictions. Failed attacks may cause a denial of service condition within the targeted delivery method. Depending on the privileges associated with the user, an attacker may install applications, view, change, or delete data or create new accounts with full user rights.

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, 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-2015-6616).

- Skia is vulnerable to memory corruption and remote code execution in a privileged process when processing a specially crafted media file (CVE-2015-6617).
- The kernel is vulnerable to a privilege escalation vulnerability that could enable a local malicious application to execute arbitrary code within the device root context (CVE-2015-6619).
- libstagefright is vulnerable to local arbitrary code execution within the context of the mediaserver service (CVE-2015-6620).
- SystemUI is vulnerable to a privilege escalation via executing a task when setting an alarm using the clock application (CVE-2015-6621).
- Native Frameworks Library is vulnerable to a security bypass (CVE-2015-6622).
- Wi-Fi is vulnerable to local arbitrary code execution within the context of an elevated system service (CVE-2015-6623).
- System Server is vulnerable to a privilege escalation vulnerability which could enable a local malicious application to gain access to service related information (CVE-2015-6624).
- System Server is vulnerable to a privilege escalation vulnerability which could enable a local malicious application to gain access to Wi-Fi service related information (CVE-2015-6625).
- libstagefright is vulnerable to a security bypass vulnerability when communicating with mediaserver (CVE-2015-6626, CVE-2015-6631, CVE-2015-6632).
- Audio is vulnerable to an information disclosure when processing a specially crafted file (CVE-2015-6627).
- Media Framework is vulnerable to a security bypass vulnerability when communicating with mediaserver (CVE-2015-6628).
- Wi-Fi is vulnerable to an information disclosure (CVE-2015-6629).
- SystemUI to an information disclosure which could enable a local malicious application to gain access to screenshots (CVE-2015-6630).
-

Successful exploitation could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, or bypassing security restrictions. Failed attacks may cause a denial of service condition within the targeted delivery method. Depending on the privileges associated with the user an attacker may install applications, view, change, or delete data, or create new accounts with full user rights.

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.
- Consider changing the default messaging application to one that has been patched and is no longer vulnerable to Stagefright.

REFERENCES:

Google:

<https://source.android.com/security/bulletin/2015-12-01.html>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6616>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6617>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6619>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6620>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6621>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6622>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6623>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6624>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6626>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6631>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6632>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6627>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6628>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6629>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6625>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6630>

TLP: WHITE

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

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