

*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:**

10/02/2015

**SUBJECT:**

Multiple Vulnerabilities in Google Stagefright Could Allow Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Google's Stagefright which could allow an attacker to execute remote code. Stagefright is a media playback library native to the Android OS which processes various media formats. Android is an operating system developed by Google for mobile phones. Successfully exploiting these issues may allow remote attackers to execute remote code on the mobile phone.

**THREAT INTELLIGENCE**

There are currently no reports of these vulnerabilities being exploited in the wild. Zimperium zLabs, discoverer of the vulnerabilities, will publish a proof-of-concept for these vulnerabilities after Google releases the patch.

**SYSTEM AFFECTED:**

- Android version 1.1 through 5.1.1

**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 remote code execution. The vulnerabilities are as follows:

- Google Stagefright 'libutils' may allow for remote code execution via a specially crafted metadata in MP3 or MP4 files (CVE-2015-6602).
- Google Stagefright 'LMY48M' may allow for remote code execution via a specially crafted metadata in MP3 or MP4 files (CVE-2015-3876).

These vulnerabilities exist in Stagefright, a media playback library which processes various media formats, and affect android devices from Android 1.1 through Android 5.1.1, and could be exploited if a user visits or is redirected to a webpage playing a specially crafted MP3 audio or MP4 video file. Zimperium originally disclosed the vulnerabilities to Google on August 15, 2015, and will disclose them to the public after the vulnerabilities have been resolved. Successfully exploiting these issues may allow remote attackers to execute remote code on the mobile phone.

#### **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 retrieve MMS messages. If your app does not support this functionality, 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.
- If your Messaging app supports it, consider blocking messages from unknown senders.
- To determine if your device is vulnerable to Stagefright 2.0, consider testing it with Zimperium's 'Stagefreight Detector' after an update is made available.

#### **REFERENCES:**

##### **Zimperium:**

<https://blog.zimperium.com/zimperium-zlabs-is-raising-the-volume-new-vulnerability-processing-mp3mp4-media/>

<https://blog.zimperium.com/stagefright-vulnerability-details-stagefright-detector-tool-released/>

##### **PCWorld:**

<http://www.pcworld.com/article/2988211/android/new-android-vulnerabilities-put-over-a-billion-devices-at-risk-of-remote-hacking.html>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6602>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3876>

#### **TLP: WHITE**

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

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