

*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:**

08/11/2015

**SUBJECT:**

Multiple Vulnerabilities in Google Stagefright Could Allow Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Stagefright, a component of Android, which could allow an attacker to execute arbitrary code. Android is an operating system developed by Google for mobile phones. Successfully exploiting these issues may allow remote attackers to execute arbitrary code on the mobile phone.

**THREAT INTELLIGENCE**

There are currently no reports of these vulnerabilities being exploited in the wild. There is a known proof-of-concept exploit for this vulnerability developed by Zimperium which is scheduled to be released to the public on August 24, 2015.

**SYSTEM AFFECTED:**

- Android version 2.2 (Froyo) and above

**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:**

Multiple vulnerabilities exist affecting Android devices that could allow for remote code execution. The vulnerabilities are in Stagefright, a media playback library native to Android that processes various media formats, and according to Zimperium "...critically expose 95% of Android devices." (Google states that 90% of Android devices have Address Space Layout Randomization (ASLR) technology enabled that help to protect them from this vulnerability.) Zimperium originally disclosed the vulnerabilities to Google in April 2015, and publicly disclosed them on July 27, 2015. Zimperium identified the vulnerabilities as:

- Google Stagefright 'stsc' MP4 Atom Integer Overflow Remote Code Execution (CVE-2015-1538, P0006).
- Google Stagefright 'ctts' MP4 Atom Integer Overflow Remote Code Execution (CVE-2015-1538, P0004).
- Google Stagefright 'stts' MP4 Atom Integer Overflow Remote Code Execution (CVE-2015-1538, P0004).
- Google Stagefright 'stss' MP4 Atom Integer Overflow Remote Code Execution (CVE-2015-1538, P0004).
- Google Stagefright 'esds' MP4 Atom Integer Underflow Remote Code Execution (CVE-2015-1539, P0007).
- Google Stagefright 'covr' MP4 Atom Integer Underflow Remote Code Execution (CVE-2015-3827, P0008).
- Google Stagefright 3GPP Metadata Buffer Overread (CVE-2015-3826, P0009).
- Google Stagefright 3GPP Integer Underflow Remote Code Execution (CVE-2015-3828, P0010).
- Google Stagefright 'tx3g' MP4 Atom Integer Overflow Remote Code Execution (CVE-2015-3824, P0011).
- Google Stagefright 'covr' MP4 Atom Integer Overflow Remote Code Execution (CVE-2015-3829, P0012).

According to Zimperium the vulnerabilities can be exploited through various methods, including sending an exploit within a Multimedia Messaging Service (MMS) message to a mobile phone number. Successful exploitation could allow for code to be executed on the targeted device, and in some cases, unbeknownst to the victim. The code could be executed and the message deleted before the victim notices the message. This exploitation would initially allow an attacker full access to anything to which Stagefright has access as a media user, including but not limited to photos, voice recordings, music, and videos. Subsequently, after applying a PE exploit, the attacker can then escalate his/her privileges to attain root access.

#### **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 so the device does not 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.

#### **REFERENCES:**

##### **Zimperium:**

<https://blog.zimperium.com/stagefright-vulnerability-details-stagefright-detector-tool-released/#sthash.Qpki14Ps.dpuf>

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

##### **NPR:**

<http://www.npr.org/sections/alltechconsidered/2015/08/05/429649509/under-pressure-google-promises-to-update-android-security-regularly>

**TLP: WHITE**

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

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