

*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:**

11/10/2015

**SUBJECT:**

Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB15-28)

**OVERVIEW:**

Multiple vulnerabilities in Adobe Flash Player could allow remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, compromising processing resources in a user's computer, or remote code execution. Failed exploit attempts will likely cause denial-of-service conditions.

**THREAT INTELLIGENCE:**

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

**SYSTEMS AFFECTED:**

- Adobe Flash Player Desktop Runtime versions prior to 19.0.0.226 for Windows and Macintosh
- Adobe Flash Player Extended Support Release versions prior to 18.0.0.255 for Windows and Macintosh
- Adobe Flash Player for Google Chrome versions prior to 19.0.0.226 for Windows, Macintosh, Linux and ChromeOS
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 versions prior to 19.0.0.226 for Windows 10
- Adobe Flash Player for Internet Explorer 10 and 11 versions prior to 19.0.0.226 for Windows 8.0 and 8.1
- Adobe Flash Player for Linux versions prior to 11.202.540 for Linux
- Adobe AIR Desktop Runtime versions prior to 19.0.0.213 for Windows and Macintosh
- Adobe Air SDK versions prior to 19.0.0.213 for Windows, Macintosh, Android, and iOS
- AIR SDK & Compiler versions prior to 19.0.0.213 for Windows, Macintosh, Android, and iOS
- AIR for Android versions prior to 19.0.0.190 for Android via Google Play

**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:**

Adobe Flash Player is prone to multiple vulnerabilities. These vulnerabilities are as follows:

- One type confusion vulnerability leading to remote code execution (CVE-2015-7659)
- Three security bypass vulnerabilities that could be exploited to write arbitrary data to the file system under user permissions (CVE-2015-7662).
- 15 use-after-free vulnerabilities that could lead to remote code execution (CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, CVE-2015-8046).

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, compromising processing resources in a user's computer, or remote code execution. Failed exploit attempts will likely cause denial-of-service conditions.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to those required only.

#### **REFERENCES:**

##### **Adobe:**

<https://helpx.adobe.com/security/products/flash-player/apsb15-28.html>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7651>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7652>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7653>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7654>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7655>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7656>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7657>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7658>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7659>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7660>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7661>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7662>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7663>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8042>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8043>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8044>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8046>

#### **TLP: WHITE**

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

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