

*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:**

09/21/2015

**SUBJECT:**

Multiple Vulnerabilities in Adobe Flash Player and Adobe AIR Could Allow for Remote Code Execution (APSB15-23)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Adobe Flash Player and Adobe AIR that 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. Adobe AIR is a cross platform runtime used for developing Internet applications that run outside of a browser. Successful exploitation of these vulnerabilities may allow for arbitrary code execution in the context of the current user. Failed exploit attempts will likely result in 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 18.0.0.232 and earlier for Windows and Macintosh
- Adobe Flash Player Extended Support Release 18.0.0.232 and earlier for Windows and Macintosh
- Adobe Flash Player for Google Chrome 18.0.0.233 and earlier for Windows, Macintosh, Linux and ChromeOS
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 18.0.0.232 and earlier for Windows 10
- Adobe Flash Player for Internet Explorer 10 and 11 18.0.0.232 and earlier for Windows 8.0 and 8.1
- Adobe Flash Player for Linux 11.2.202.508 and earlier for Linux
- AIR Desktop Runtime 18.0.0.199 and earlier for Windows and Macintosh
- AIR SDK 18.0.0.199 and earlier for Windows, Macintosh, Android and iOS
- AIR SDK & Compiler 18.0.0.180 and earlier for Windows, Macintosh, Android and iOS
- AIR for Android 18.0.0.143 and earlier for Android

**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 and Adobe AIR are prone to multiple vulnerabilities which could allow for remote code execution. These vulnerabilities are as follows:

- A type confusion vulnerability that could lead to code execution (CVE-2015-5573).
- Multiple use-after-free vulnerabilities could lead to code execution (CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, CVE-2015-5584, CVE-2015-6682).
- Multiple buffer overflow vulnerabilities that could lead to code execution (CVE-2015-6676, CVE-2015-6678).
- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, CVE-2015-6677).
- Additional validation checks ensure that Flash Player rejects malicious content from vulnerable JSONP callback APIs (CVE-2015-5571).
- A memory leak vulnerability (CVE-2015-5576).
- Further hardening to a mitigation to defend against vector length corruptions (CVE-2015-5568).
- Multiple stack corruption vulnerabilities that could lead to code execution (CVE-2015-5567, CVE-2015-5579).
- A stack overflow vulnerability that could lead to code execution (CVE-2015-5587).
- A security bypass vulnerability that could lead to information disclosure (CVE-2015-5572).
- A vulnerability that could be exploited to bypass the same-origin-policy and lead to information disclosure (CVE-2015-6679).

Successful exploitation of these vulnerabilities may allow for arbitrary code execution in the context of the current user. Failed exploit attempts will likely result in 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/apsb15-23.html>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5567>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5568>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5570>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5571>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5572>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5573>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5574>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5575>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5576>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5577>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5578>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5579>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5580>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5581>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5582>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5584>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5587>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5588>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6676>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6677>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6678>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6679>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6682>

**TLP: WHITE**

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

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