

*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:**

06/09/2015

**SUBJECT:**

Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB15-11)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Adobe Flash Player, a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages.

Successful exploitation of these vulnerabilities could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer.

**THREAT INTELLIGENCE**

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

**SYSTEM AFFECTED:**

- . Adobe Flash Player prior to version 18.0.0.160
- . Adobe Flash Player Extended Support Release prior to version 13.0.0.292
- . Adobe Flash Player prior to version 11.2.202.466 for Linux
- . Adobe AIR Desktop Runtime prior to version 18.0.0.143 for Macintosh
- . Adobe AIR Desktop Runtime prior to version 18.0.0.144 for Windows
- . Adobe AIR SDK and SDK & Compiler prior to version 18.0.0.143 for Macintosh
- . Adobe AIR SDK and SDK & Compiler prior to version 18.0.0.144 for Windows
- . Adobe AIR for Android prior to version 18.0.0.143

**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:

- . Integer overflow vulnerability that could lead to code execution (CVE-2015-3104)
- . Memory corruption vulnerability that could lead to code execution (CVE-2015-3105)
- . Multiple use-after-free vulnerability that could lead to code execution (CVE-2015-3103, CVE-2015-3106, CVE-2015-3107)
- . Stack overflow vulnerability that could lead to code execution (CVE-2015-3100)
- . A vulnerability that could be exploited to bypass the fix for CVE-2014-5333 (CVE-2015-3096)

- Multiple vulnerabilities that could be exploited to bypass the same-origin-policy and lead to information disclosure (CVE-2015-3098, CVE-2015-3099, CVE-2015-3102)
- Memory leak vulnerability that could be used to bypass ASLR (CVE-2015-3108)
- Permission issues in Flash broker for Internet Explorer that could be exploited to perform privilege escalation (CVE-2015-3101)
- These updates improve memory address randomization of Flash heap for Windows 7 64-bit (CVE-2015-3097)

Successful exploitation of these vulnerabilities could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.

#### **REFERENCES:**

##### **Adobe:**

<https://helpx.adobe.com/security/products/flash-player/apsb15-11.html>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3096>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3097>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3098>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3099>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3100>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3101>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3102>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3103>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3104>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3105>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3106>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3107>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3108>

#### **TLP: WHITE**

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

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