

*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:**

02-09-2016

**SUBJECT:**

Multiple Vulnerabilities in Adobe Products Could Allow for Remote Code Execution (APSB16-03, 04, 05, 07)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Adobe Connect, Experience Manager, Flash Player and Photoshop CC that could allow for remote code execution. Adobe Connect is software used to create information and general presentations, online training materials, web conferencing, learning modules, and user desktop sharing. Adobe Experience Manager is a Web Content Management System designed to enable users to create, edit, manage and optimize websites across different digital channels such as web and mobile. Adobe Photoshop CC is a graphics editor program. 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 of these vulnerabilities may allow for remote code execution in the context of the current user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE**

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

**SYSTEMS AFFECTED:**

- Adobe Flash Player Desktop Runtime prior to 20.0.0.286 for Windows and Macintosh
- Adobe Flash Player Extended Support Release prior to 18.0.0.326 for Windows and Macintosh
- Adobe Flash Player for Google Chrome prior to 20.0.0.286 for Windows, Macintosh, Linux and ChromeOS
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 prior to 20.0.0.272 for Windows 10
- Adobe Flash Player for Internet Explorer 11 prior to 20.0.0.272 for Windows 8.1
- Adobe Flash Player for Linux prior to 11.2.202.559 for Linux
- AIR Desktop Runtime prior to 20.0.0.233 for Windows and Macintosh
- AIR SDK prior to 20.0.0.233 for Windows, Macintosh, Android and iOS
- AIR SDK & Compiler prior to 20.0.0.233 for Windows, Macintosh, Android and iOS
- Adobe Photoshop CC prior to 16.1.1 for Windows and Macintosh
- Adobe Bridge CC prior to 6.1.1 for Windows and Macintosh
- Adobe Experience Manager 5.6.1, 6.1.0, 6.0.0 for Windows, Unix, Linux, and OS X

- Adobe Connect prior to 9.4.2 for Windows

**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: Medium****TECHNICAL SUMMARY:**

Adobe Connect, Experience Manager, Flash Player and Photoshop CC are prone to multiple vulnerabilities, the most severe of which could allow for remote code execution. These vulnerabilities are as follows:

- A type confusion vulnerability that may lead to code execution (CVE-2016-0985).
- Multiple use-after-free vulnerabilities could lead to code execution (CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, CVE-2016-0983, CVE-2016-0984).
- A heap buffer overflow vulnerability that could lead to code execution (CVE-2016-0971).
- Multiple memory corruption vulnerabilities that may lead to code execution (CVE-2016-0951, CVE-2016-0952, CVE-2016-0953, CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, CVE-2016-0981).
- A Java deserialization issue (CVE-2016-0958).
- A cross-site scripting vulnerability that could lead to information disclosure (CVE-2016-0955).
- An information disclosure vulnerability affecting Apache Sling Servlets Post 2.3.6 (CVE-2016-0956).
- A URL filter bypass vulnerability that could be used to circumvent dispatcher rules (CVE-2016-0957).
- A cross-site request forgery protection feature (CVE-2016-0948).
- An input validation vulnerability (CVE-2016-0949).
- A content spoofing vulnerability (CVE-2016-0950).

Successful exploitation of these vulnerabilities could allow for remote code execution in the context of the current user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**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.
- Limit user account privileges to those required only.
- Do not open email attachments from unknown or untrusted sources.

## REFERENCES:

### Adobe:

<https://helpx.adobe.com/security/products/photoshop/apsb16-03.html>  
<https://helpx.adobe.com/security/products/flash-player/apsb16-04.html>  
<https://helpx.adobe.com/security/products/experience-manager/apsb16-05.html>  
<https://helpx.adobe.com/security/products/connect/apsb16-07.html>

### CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0948>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0949>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0950>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0951>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0952>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0953>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0955>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0956>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0957>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0958>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0964>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0965>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0966>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0967>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0968>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0969>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0970>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0971>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0972>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0973>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0974>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0975>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0976>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0977>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0978>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0979>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0980>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0981>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0982>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0983>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0984>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0985>

### TLP: WHITE

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

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