

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:

05/10/2016

05/12/2016 - UPDATED

SUBJECT:

A Vulnerability in Adobe Flash Player Could Allow for Remote Code Execution (APSA16-02)

May 12 – UPDATED SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSA16-02, APSA16-15)

OVERVIEW:

A vulnerability has been discovered in Adobe Flash Player which could allow for 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 of this vulnerability may allow for remote code execution and allow an attacker to take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights with failed exploit attempts will likely result in denial-of-service conditions.

May 12 – UPDATED OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow for remote code execution.

THREAT INTELLIGENCE:

Adobe is aware of a report that an exploit for CVE-2016-4117 exists in the wild.

SYSTEM AFFECTED:

- Adobe Flash Player 21.0.0.226 and earlier for Windows, Macintosh, Linux, and Chrome OS

May 12 – UPDATED SYSTEMS AFFECTED:

- **Adobe Flash Player Desktop Runtime prior to 21.0.0.242 for Windows and Macintosh**
- **Adobe Flash Player Extended Support Release prior to 18.0.0.352 for Windows and Macintosh**
- **Adobe Flash Player for Google Chrome prior to 21.0.0.242 for Windows, Macintosh, Linux and ChromeOS**
- **Adobe Flash Player for Microsoft Edge and Internet Explorer 11 prior to 21.0.0.242 for Windows 8.1 and 10**
- **Adobe Flash Player for Linux prior to 11.2.202.621 for Linux**
- **AIR Desktop Runtime prior to 21.0.0.215 for Windows and Macintosh**

- *AIR SDK prior to 21.0.0.215 for Windows, Macintosh, Android and iOS*
- *AIR SDK & Compiler prior to 21.0.0.215 for Windows, Macintosh, Android and iOS*

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

An unspecified security vulnerability has been discovered in Adobe Flash Player which could allow for remote code execution.

Successful exploitation of this vulnerability may allow for remote code execution and allow an attacker to take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights with failed exploit attempts will likely result in denial-of-service conditions.

May 12 – UPDATED TECHNICAL SUMMARY:

Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution.

These vulnerabilities are as follows:

- ***Multiple type confusion vulnerabilities could lead to remote code execution. (CVE-2016-1105, CVE-2016-4117)***
- ***Multiple use-after-free vulnerabilities could lead to remote code execution. (CVE-2016-1097, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, CVE-2016-4110).***
- ***A heap buffer overflow vulnerability that could lead to remote code execution. (CVE-2016-1101).***
- ***A buffer overflow vulnerability that could lead to remote code execution. (CVE-2016-1103).***
- ***Multiple memory corruption vulnerabilities that could lead to remote code execution. (CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115).***
- ***A directory search path vulnerability that could lead to remote code execution. (CVE-2016-4116).***

Successful exploitation of these vulnerabilities may allow for remote code execution and allow an attacker to take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights with failed exploit attempts will likely result in denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Disable Flash functionality until a patch is released by Adobe.

- 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.

May 12 - UPDATED RECOMMENDATIONS:

We recommend the following actions be taken:

- **Install the updates provided by Adobe immediately after appropriate testing.**

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/flash-player/apsa16-02.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4117>

May 12 – UPDATED REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/flash-player/apsb16-15.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1096>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1097>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1098>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1099>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1100>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1101>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1102>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1103>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1104>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1105>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1106>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1107>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1108>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1109>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1110>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4108>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4109>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4110>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4111>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4112>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4113>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4114>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4115>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4116>

TLP: WHITE

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

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