

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:

12/28/2015

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player and AIR Could Allow Remote Code Execution (APSB16-01)

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 is a report of a CVE-2015-8651 exploit utilized in limited attacks.

SYSTEMS AFFECTED:

- Adobe Flash Player Desktop Runtime prior to 20.0.0.267 for Windows and Macintosh
- Adobe Flash Player Extended Support Release prior to 18.0.0.324 for Windows and Macintosh
- Adobe Flash Player for Google Chrome prior to 20.0.0.267 for Windows, Macintosh, Linux and ChromeOS
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 prior to 20.0.0.267 for Windows 10
- Adobe Flash Player for Internet Explorer 10 and 11 prior to 20.0.0.267 for Windows 8.0 and 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
- AIR for Android prior to 20.0.0.233 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 may lead to code execution (CVE-2015-8644).
- Multiple use-after-free vulnerabilities could lead to code execution (CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, CVE-2015-8650).
- An integer overflow vulnerability that may lead to code execution (CVE-2015-8651).
- Multiple memory corruption vulnerabilities that may lead to code execution (CVE-2015-8459, CVE-2015-8460, CVE-2015-8636, CVE-2015-8645).

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/apsb16-01.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8459>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8460>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8634>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8635>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8636>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8638>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8639>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8640>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8641>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8642>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8643>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8644>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8645>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8646>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8647>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8648>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8649>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8650>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8651>

TLP: WHITE

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

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