

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:

10/13/2015

10/15/2015 - Updated

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB15-25)

OVERVIEW:

Multiple vulnerabilities in Adobe Flash Player 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. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, compromising processing resources in a user's computer, or remote code execution. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE

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

October 15 – UPDATED THREAT INTELLIGENCE

Adobe is aware of a report that an exploit for the CVE-2015-7645 critical vulnerability is being used in limited, targeted attacks.

SYSTEM AFFECTED:

- Adobe Flash Player Desktop Runtime version 19.0.0.185 and earlier and earlier for Windows and Macintosh
- Adobe Flash Player Extended Support Release version 19.0.0.185 and earlier and earlier for Windows and Macintosh
- Adobe Flash Player for Google Chrome version 19.0.0.185 and earlier for Windows, Macintosh, Linux and ChromeOS
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 version 19.0.0.185 and earlier for Windows 10
- Adobe Flash Player for Internet Explorer 10 and 11 version 19.0.0.185 and earlier for Windows 8.0 and 8.1
- Adobe Flash Player for Linux version 11.2.202.521 and earlier for Linux
- Adobe AIR Desktop Runtime version 19.0.0.190 and earlier for Windows and Macintosh
- Adobe Air SDK version 19.0.0.190 and earlier for Windows, Macintosh, Android, and iOS
- AIR SDK & Compiler version 19.0.0.190 and earlier for Windows, Macintosh, Android, and iOS

October 15 – UPDATED SYSTEM AFFECTED:

- **Adobe Flash Player 19.0.0.207 and earlier versions for Windows and Macintosh**
- **Adobe Flash Player Extended Support Release version 18.0.0.252 and earlier 18.x versions**
- **Adobe Flash Player 11.2.202.535 and earlier 11.x versions for Linux**

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:

- A vulnerability that could be exploited to bypass the same-origin-policy and lead to information disclosure (CVE-2015-7628).
- A defense-in-depth feature in the Flash broker API (CVE-2015-5569).
- A use-after-free vulnerabilities that could lead to code execution (CVE-2015-7629, CVE-2015-7631, CVE-2015-7643, CVE-2015-7644).
- A buffer overflow vulnerability that could lead to code execution (CVE-2015-7632).
- Memory corruption vulnerabilities that could lead to code execution (CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, CVE-2015-7634).

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, compromising processing resources in a user's computer, or remote code execution. Failed exploit attempts will likely cause denial-of-service conditions.

October 15 – UPDATED TECHNICAL SUMMARY:

- **Multiple use-after-free vulnerabilities that could lead to code execution (CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, CVE-2015-7644).**
- **A critical vulnerability that could cause a crash and allow an attacker to take control of the affected system (CVE-2015-7645).**

Please note Adobe Flash Player 19.0.0.207, 18.0.0.252 and 11.2.202.535 are still vulnerable to CVE-2015-7645. Adobe expects to release another patch for CVE-2015-7645 during the week of October 19.

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/apsb15-25.html>

CVE

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7628>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5569>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7629>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7631>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7643>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7644>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7632>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7625>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7626>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7627>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7630>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7633>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7634>

October 15 – UPDATED REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/flash-player/apsa15-05.html>

Trend Micro:

<http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7635>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7636>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7637>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7638>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7639>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7640>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7641>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7642>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7645>

TLP: WHITE

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

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