

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:

08/11/2015

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB15-19)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player, which could allow arbitrary 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 these vulnerabilities could result in an attacker executing arbitrary code in the context of the user running the affected applications. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. A failed exploit attempt could create a denial-of-service attack.

THREAT INTELLIGENCE:

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

SYSTEM AFFECTED:

- Adobe Flash Player Desktop Runtime 18.0.0.209 and earlier for Windows and Mac
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 18.0.0.209 and earlier for Windows 10
- Adobe Flash Player for Internet Explorer 10 and 11 18.0.0.209 and earlier for Windows 8.0 and 8.1
- Adobe Flash Player Extended Support Release 13.0.0.309 and earlier for Windows and Macintosh
- Adobe Flash Player for Google Chrome 18.0.0.209 and earlier for Windows, Macintosh and Linux
- Adobe Flash Player for Linux 11.2.202.491 and earlier Linux
- AIR Desktop Runtime 18.0.0.180 and earlier for Windows and Macintosh
- AIR SDK 18.0.0.180 and earlier for Windows, Mac, Android and iOS
- AIR SDK & Compiler 18.0.0.180 and earlier 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:

Adobe Flash Player is prone to multiple vulnerabilities. These vulnerabilities are as follows:

- Multiple type confusion vulnerabilities that could lead to code execution (CVE-2015-5128, CVE-2015-5554, CVE-2015-5555, CVE-2015-5558, CVE-2015-5562).
- A vector length corruption issue that was originally addressed in version 18.0.0.209 (CVE-2015-5125).
- Multiple use-after-free vulnerabilities that could lead to code execution (CVE-2015-5550, CVE-2015-5551, CVE-2015-3107, CVE-2015-5556, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5557, CVE-2015-5559, CVE-2015-5127, CVE-2015-5563, CVE-2015-5561, CVE-2015-5124).
- Multiple heap buffer overflow vulnerabilities that could lead to code execution (CVE-2015-5129, CVE-2015-5541).
- Multiple buffer overflow vulnerabilities that could lead to code execution (CVE-2015-5131, CVE-2015-5132, CVE-2015-5133).
- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, CVE-2015-5553).
- An integer overflow vulnerability that could lead to code execution (CVE-2015-5560).

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights as the logged on 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

Update immediately after appropriate testing.

- Apply appropriate patches provided by Adobe to vulnerable systems immediately after appropriate testing.
- 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 from un-trusted sources.

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/flash-player/apsb15-19.html>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-3107>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5124>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5125>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5127>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5128>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5129>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5130>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5131>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5132>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5133>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5134>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5539>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5540>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5541>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5544>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5545>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5546>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5547>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5548>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5549>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5550>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5551>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5552>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5553>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5554>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5555>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5556>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5557>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5558>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5559>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5560>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5561>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5562>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-5563>

TLP: WHITE

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

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