

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:

04/14/2015

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB15-06)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player. 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 compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer.

THREAT INTELLIGENCE:

Adobe has reported that an exploit for CVE-2015-3043 exists in the wild. There are currently no reports of the other vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Adobe Flash Player 17.0.0.134 and earlier versions
- Adobe Flash Player 13.0.0.277 and earlier 13.x versions
- Adobe Flash Player 11.2.202.451 and earlier 11.x versions

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 memory corruption vulnerabilities that could lead to remote code execution (CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, CVE-2015-3043).
- Type confusion vulnerability that could lead to remote code execution (CVE-2015-0356).
- Buffer overflow vulnerability that could lead to remote code execution (CVE-2015-0348).
- Use-after-free vulnerabilities that could lead to remote code execution (CVE-2015-0349, CVE-2015-0351, CVE-2015-0358, CVE-2015-3039).
- Double-free vulnerabilities that could lead to remote code execution (CVE-2015-0346, CVE-2015-0359).

- Memory leak vulnerabilities that could be used to bypass Address Space Layout Randomization (ASLR) (CVE-2015-0357, CVE-2015-3040).
- Security bypass vulnerability that could lead to information disclosure (CVE-2015-3044).

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:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit untrusted 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.
- Adobe Flash Player installed with Google Chrome, as well as Internet Explorer on Windows 8.x, will automatically update to version 17.0.0.169 when available.

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/flash-player/apsb15-06.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0346>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0347>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0348>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0349>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0350>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0351>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0352>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0353>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0354>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0355>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0356>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0357>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0358>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0359>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0360>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0338>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0339>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0340>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0341>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0342>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0343>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0344>

TLP: WHITE

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

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