

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.

DATE(S) ISSUED:

06/10/2014

SUBJECT:

Security Updates for Multiple Vulnerabilities in Adobe Flash Player (APSB14-16)

EXECUTIVE SUMMARY:

A security update has been released to address multiple vulnerabilities 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 this vulnerability could result in an attacker gaining the same privileges 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. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- Adobe Flash Player 13.0.0.214 and earlier versions for Windows
- Adobe Flash Player 13.0.0.214 and earlier versions for Macintosh
- Adobe Flash Player 11.2.202.359 and earlier 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:

A security update has been released to address multiple vulnerabilities in Adobe Flash Player. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage, or opens a specially crafted file. This security update addresses the following vulnerabilities:

- Multiple cross-site scripting vulnerabilities (CVE-2014-0531, CVE-2014-0532, CVE-2014-0533).
- Multiple security bypass vulnerabilities (CVE-2014-0534, CVE-2014-0535).
- A memory corruption vulnerability that could result in arbitrary code execution (CVE-2014-0536).

Successful exploitation of these vulnerabilities could result in an attacker taking control of an affected machine.

To verify the version of Adobe Flash Player installed on your system, access the About Flash Player page ([www.\[.\]adobe.\[.\]com/products/flash/about](http://www.adobe.com/products/flash/about)), or right-click on content running in Flash Player and select “About Adobe (or Macromedia) Flash Player” from the menu. If you use multiple browsers, perform the check for each browser you have installed on your system to determine if one is using a vulnerable version of Flash.

RECOMMENDATIONS:

The following actions should be taken:

- 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.

REFERENCES:

Adobe:

<http://helpx.adobe.com/security/products/flash-player/apsb14-16.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0531>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0532>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0533>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0534>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0535>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0536>