

*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:**

03/11/2014

**SUBJECT:**

Multiple Vulnerabilities Discovered in Adobe Flash Player (APSB14-08)

**EXECUTIVE SUMMARY:**

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

**THREAT INTELLIGENCE:**

At this time these vulnerabilities are not publicly disclosed and there is no known proof-of-concept code available.

**SYSTEMS AFFECTED:**

- Adobe Flash Player 12.0.0.70 and earlier versions for Windows and Macintosh
- Adobe Flash Player 11.2.202.341 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:**

Adobe Flash Player is prone to multiple vulnerabilities. Specifically, the vulnerabilities identified may allow an attacker to bypass the same origin policy or read the contents of the clipboard. Failed exploitation attempts may cause denial-of-service conditions. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. Failed exploit attempts will likely cause 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 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/apsb14-08.html>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0503>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0504>