

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:

07/08/2014

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player and Adobe AIR Could Allow Remote Code Execution (APSB14-17)

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Adobe Flash Player and Adobe AIR. 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. Adobe AIR is a cross platform runtime used for developing Internet applications that run outside of a browser. 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:

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

SYSTEMS AFFECTED:

- Adobe Flash Player 14.0.0.125 and earlier versions for Windows and Macintosh
- Adobe Flash Player 11.2.202.378 and earlier versions for Linux
- Adobe AIR 14.0.0.110 SDK and earlier versions
- Adobe AIR 14.0.0.110 SDK & Compiler and earlier versions
- Adobe AIR 14.0.0.110 and earlier versions for Android

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 and AIR are prone to multiple vulnerabilities. Specifically, the vulnerabilities identified may allow an attacker to run malicious code through exploiting vulnerable JSONP callback APIs or through multiple security bypass vulnerabilities. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources on 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.
- Limit user account privileges to those required only.

REFERENCES:**Adobe:**

<http://helpx.adobe.com/security/products/flash-player/apsb14-17.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4671>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0537>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0539>