

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:

11/11/2014

SUBJECT:

Multiple vulnerabilities found in Adobe Flash Player Could Allow Remote Code Execution (APSB14-24)

EXECUTIVE SUMMARY:

Multiple vulnerabilities in Adobe Flash Player and Adobe AIR could allow remote 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. 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.

SYSTEM AFFECTED:

Adobe Flash Player 15.0.0.189 and earlier versions
Adobe Flash Player 13.0.0.250 and earlier 13.x versions
Adobe Flash Player 11.2.202.411 and earlier versions for Linux
Adobe AIR desktop runtime 15.0.0.293 and earlier versions
Adobe AIR SDK 15.0.0.302 and earlier versions
Adobe AIR SDK & Compiler 15.0.0.302 and earlier versions
Adobe AIR 15.0.0.293 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 is prone to multiple vulnerabilities that could allow for remote code execution. These vulnerabilities are as follows:

Memory corruption vulnerabilities that could lead to code execution (CVE-2014-0576, CVE-2014-0581, CVE-2014-8440, CVE-2014-8441)

Use-after-free vulnerabilities that could lead to code execution (CVE-2014-0573, CVE-2014-0588, CVE-2014-8438).

A double free vulnerability that could lead to code execution (CVE-2014-0574).

Type confusion vulnerabilities that could lead to code execution (CVE-2014-0577, CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, CVE-2014-0590).

Heap buffer overflow vulnerabilities that could lead to code execution (CVE-2014-0582, CVE-2014-0589).

Information disclosure vulnerability that could be exploited to disclose session tokens (CVE-2014-8437).

Heap buffer overflow vulnerability that could be exploited to perform privilege escalation from low to medium integrity level (CVE-2014-0583).

A permission issue that could be exploited to perform privilege escalation from low to medium integrity level (CVE-2014-8442).

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.

RECOMMENDATIONS:

The following actions should be taken:

Install the updates provided by Adobe immediately after appropriate testing.

Remind users not to visit 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/apsb14-24.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0573>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0574>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0576>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0577>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0581>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0582>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0583>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0584>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0585>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0586>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0588>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0590>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8437>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8438>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8440>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8441>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8442>