

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:

11/06/2012

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB12-24)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow attackers to take complete control of affected systems. 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 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

SYSTEMS AFFECTED:

- Adobe Flash Player 11.4.402.287 and earlier versions for Windows
- Adobe Flash Player 11.4.402.287 and earlier versions for Macintosh
- Adobe Flash Player 11.2.202.243 and earlier versions for Linux
- Adobe Flash Player 11.1.115.20 and earlier versions for Android 4.x
- Adobe Flash Player 11.1.111.19 and earlier versions for Android 3.x and 2.x
- Flash Player 11.4.402.287 and earlier for Chrome users
- Flash Player 11.3.375.10 and earlier in Internet Explorer 10
- Adobe AIR 3.4.0.2710 and earlier versions for Windows and Macintosh
- Adobe 3.4.0.2710 SDK (includes AIR for iOS) and earlier versions
- Adobe AIR 3.4.0.2710 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

DESCRIPTION:

Adobe Flash Player is prone to twenty-four vulnerabilities that could allow for remote code execution. The vulnerabilities are as follows:

- Multiple buffer overflow vulnerabilities that could lead to code execution (CVE-2012-5274, CVE-2012-5275, CVE-2012-5276, CVE-2012-5277, CVE-2012-5280).
- A memory corruption vulnerability that could lead to code execution (CVE-2012-5279)
- A security bypass vulnerability that could lead to code execution (CVE-2012-5278).

Successful exploitation 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.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Users of Adobe Flash Player 11.4.402.287 and earlier versions for Windows and Macintosh should update to Adobe Flash Player 11.5.502.110.
- Users of Adobe Flash Player 11.2.202.243 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.251.
- Flash Player installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 11.5.31.2 for Windows, Macintosh and Linux.
- Flash Player installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 11.3.376.12 for Windows.
- Users of Adobe Flash Player 11.1.115.20 and earlier versions on Android 4.x devices should update to Adobe Flash Player 11.1.115.27.
- Users of Adobe Flash Player 11.1.111.19 and earlier versions for Android 3.x and earlier versions should update to Flash Player 11.1.111.24.
- Users of Adobe AIR 3.4.0.2710 for Windows and Macintosh, SDK (including AIR for iOS) and Android should update to Adobe AIR 3.5.0.600.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- 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://www.adobe.com/support/security/bulletins/apsb12-24.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5274>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5275>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5276>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5277>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5278>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5279>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5280>