

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:

10/8/2012

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player and AIR Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player and Adobe AIR that could allow attackers to take complete control of affected systems. Adobe Flash Player and Adobe AIR are widely distributed multimedia's and application players 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 11.4.402.278 and earlier versions for Windows
Adobe Flash Player 11.4.402.265 and earlier versions for Macintosh
Adobe Flash Player 11.2.202.238 and earlier versions for Linux
Adobe Flash Player 11.1.115.17 and earlier versions for Android 4.x
Adobe Flash Player 11.1.111.16 and earlier versions for Android 3.x and 2.x
Adobe AIR 3.4.0.2540 and earlier versions for Windows and Macintosh
Adobe AIR 3.4.0.2540 SDK (includes AIR for iOS) and earlier versions
Adobe AIR 3.4.0.2540 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 memory-corruption vulnerabilities that may result in code-execution. (CVE-2012-5252, CVE-2012-5256, CVE-2012-5258, CVE-2012-5261, CVE-2012-5263, CVE-2012-5267, CVE-2012-5268, CVE-2012-5269, CVE-2012-5270, CVE-2012-5271, CVE-2012-5272)

Multiple buffer-overflow vulnerability that may result in code-execution. (CVE-2012-5248, CVE-2012-5249, CVE-2012-5250, CVE-2012-5251, CVE-2012-5253, CVE-2012-5254)

5254, CVE-2012-5255, CVE-2012-5257, CVE-2012-5259, CVE-2012-5260, CVE-2012-5262, CVE-2012-5264, CVE-2012-5265, CVE-2012-5266)

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 11.4.402.278 and earlier versions for Windows and Adobe Flash Player 11.4.402.265 and earlier versions for Macintosh should update to Adobe Flash Player 11.4.402.287.
- Users of Adobe Flash Player 11.2.202.238 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.243.
- Flash Player installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 11.4.31.110 for Windows and Linux, and Flash Player 11.4.402.287 for Macintosh.
- Flash Player installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 11.3.375.10 for Windows.
- Users of Adobe Flash Player 11.1.115.17 and earlier versions on Android 4.x devices should update to Adobe Flash Player 11.1.115.20.
- Users of Adobe Flash Player 11.1.111.16 and earlier versions for Android 3.x and earlier versions should update to Flash Player 11.1.111.19.
- Users of Adobe AIR 3.4.0.2540 for Windows and Macintosh should update to Adobe AIR 3.4.0.2710.
- Users of the Adobe AIR 3.4.0.2540 SDK (includes AIR for iOS) should update to the Adobe AIR 3.4.0.2710 SDK.
- Users of the Adobe AIR 3.4.0.2540 and earlier versions for Android should update to the Adobe AIR 3.4.0.2710.
- 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/apsb12-22.html>

SecurityFocus:

<http://www.securityfocus.com/bid/55827>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5248>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5249>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5250>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5251>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5252>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5253>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5254>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5255>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5256>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5257>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5258>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5259>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5260>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5261>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5262>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5263>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5264>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5265>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5266>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5267>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5268>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5269>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5270>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5271>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5272>