

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:

09/26/2012

SUBJECT:

Vulnerability in Adobe Flash Player Could Allow For Remote Code Execution (APSB12-19)

OVERVIEW:

A vulnerability has been discovered in Adobe Flash Player that could allow an attacker to take control of the affected system. 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.

A working commercial exploit is available through VUPEN Security - Exploit and PoCs Service. This exploit is not otherwise publicly available or known to be circulating in the wild.

SYSTEMS AFFECTED:

- Adobe Flash Player 11.3.300.271 and earlier versions for Windows and Macintosh operating systems
- Adobe Flash Player 11.2.202.236 and earlier versions for Linux operating system
- Adobe Flash Player 11.1.115.11 and earlier versions for Android 4.x
- Adobe Flash Player 11.1.111.10 and earlier versions for Android 3.x and 2.x
- Adobe AIR 3.3.0.3670 and earlier versions for Windows and Macintosh
- Adobe AIR 3.3.0.3690 SDK (includes AIR for iOS) and earlier versions
- Adobe AIR 3.3.0.3650 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 a vulnerability that could allow for remote code execution. The updates available from Adobe will resolve the following:

- Memory corruption vulnerabilities that could lead to code execution (CVE-2012-4163, CVE-2012-4164, CVE-2012-4165, CVE-2012-4166).

- An integer overflow vulnerability that could lead to code execution (CVE-2012-4167).
- A cross-domain information leak vulnerability (CVE-2012-4168).
- The possibility of a crash caused by a logic error involving multiple dialogs in Firefox (CVE-2012-4171).
- A Matrix3D integer overflow vulnerability that could lead to code execution (CVE-2012-5054).

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.

Flash Player installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 11.3.31.230 for Windows and Linux, and Flash Player 11.4.402.265 for Macintosh.

A working commercial exploit is available through VUPEN Security - Exploit and PoCs Service. This exploit is not otherwise publicly available or known to be circulating in the wild.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Users of Adobe Flash Player 11.3.300.271 and earlier versions for Windows and Macintosh should update to the newest version 11.4.402.265.
- Users of Adobe Flash Player 11.2.202.236 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.238.
- Users of Adobe Flash Player 11.1.115.11 and earlier versions on Android 4.x devices should update to Adobe Flash Player 11.1.115.17.
- Users of Adobe Flash Player 11.1.111.10 and earlier versions for Android 3.x and earlier versions should update to Flash Player 11.1.111.16.
- Users of Flash Player 11.3.300.271 and earlier versions for Windows and Macintosh, who cannot update to Flash Player 11.4.402.265, Adobe has made available the update Flash Player 10.3.183.23.
- Users of Flash Player 11.2.202.236 and earlier versions for Linux, who cannot update to Flash Player 11.2.202.238, Adobe has made available the update Flash Player 10.3.183.23.
- Users of Adobe AIR 3.3.0.3670 for Windows and Macintosh should update to Adobe AIR 3.4.0.2540.
- Users of the Adobe AIR 3.3.0.3690 SDK (includes AIR for iOS) should update to the Adobe AIR 3.4.0.2540 SDK.
- Users of the Adobe AIR 3.3.0.3650 and earlier versions for Android should update to the Adobe AIR 3.4.0.2540.
- 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/apsb12-19.html>

Secunia:

<http://secunia.com/advisories/50354/>

SecurityFocus:

<http://www.securityfocus.com/bid/55691>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5054>