

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:

08/14/2012

SUBJECT:

Vulnerability in Adobe Flash Player Could Allow For Remote Code Execution (APSB12-18)

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.

This vulnerability is being actively exploited in the wild, in targeted attacks, against ActiveX versions of Flash Player for Internet Explorer on Microsoft Windows via malicious Word Documents.

SYSTEMS AFFECTED:

Adobe Flash Player 11.3.300.270 and earlier versions for Windows and Macintosh
Adobe Flash Player 11.2.202.236 and earlier for Linux
Google Chrome versions before 21.0.1180.79

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. 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 be updated automatically, so no user action is required. Google Chrome users can verify that they have updated to Google Chrome version 21.0.1180.79, which includes the latest version of Adobe Flash Player.

This vulnerability is being actively exploited in the wild, in targeted attacks, against ActiveX versions of Flash Player for Internet Explorer on Microsoft Windows via malicious Word Documents.

RECOMMENDATIONS:

The following actions should be taken:

Install the updates provided by Adobe immediately after appropriate testing.

Users of Adobe Flash Player 11.3.200.270 and earlier versions for Windows and Macintosh should update to Adobe Flash Player 11.3.300.271.

Users of Adobe Flash Player 11.2.202.236 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.238.

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/apsb12-18.html>

Secunia:

<http://secunia.com/advisories/50285/>

SecurityFocus:

<http://www.securityfocus.com/bid/55009>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1535>