

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:

5/04/2012

SUBJECT:

Adobe Flash Player Object Confusion Remote Code Execution Vulnerability (APSB12-09)

OVERVIEW:

A vulnerability has 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.

It should be noted that this vulnerability is currently being used to exploit Internet Explorer users on Windows operating systems.

SYSTEMS AFFECTED:

Adobe Flash Player 11.2.202.233 and earlier versions for Windows, Macintosh, Linux, and Solaris

Adobe Flash Player 11.1.115.7 and earlier versions for Android 4.x

Adobe Flash Player 11.1.111.8 and earlier versions for Android 3.x and 2.x

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 an object confusion vulnerability which could allow for remote code execution. An unspecified object confusion vulnerability exists due to the way the application handles URL security domain checking. Successful exploitation of this vulnerability 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 result in denial-of-service conditions.

It should be noted that this vulnerability is currently being used to exploit Internet Explorer users on Windows operating systems.

RECOMMENDATIONS:

The following actions should be taken:

Install the update from Adobe immediately after appropriate testing.

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

Do not open email attachments from unknown or untrusted sources.

Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb12-09.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0779>

ZDNet:

<http://www.zdnet.com/blog/security/adobe-warns-flash-player-malware-hitting-ie-on-windows-users/11893>