

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:

09/21/2011

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB11-26)

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 will cause the application to crash and could also 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.

There are reports that one of these vulnerabilities is being exploited in the wild in active targeted attacks designed to trick the user into clicking on a malicious link delivered in an email message.

SYSTEMS AFFECTED:

- Adobe Flash Player 10.3.183.7 and earlier versions for Windows, Macintosh, Linux and Solaris
- Adobe Flash Player for Android 10.3.186.6 and earlier versions

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:

Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:

- A universal cross-site scripting issue that could be used to take actions on a user's behalf on any website or webmail provider if the user visits a malicious website. There are reports that this vulnerability is being exploited in the wild in active targeted attacks designed to trick the user into clicking on a malicious link delivered in an email message.
- AVM stack overflow issue that may allow for remote code execution or denial of service.
- A security control bypass that could allow information disclosure.
- A streaming media logic error vulnerability that could lead to code execution.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by 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 or click on URLs from unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb11-26.html>

Security Focus:

<http://www.securityfocus.com/bid/49710>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2426>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2427>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2428>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2429>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2430>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2444>