

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:

05/08/2012

SUBJECT:

Multiple Vulnerabilities in Adobe Shockwave Player Could Allow For Code Execution (APSB12-13)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Shockwave, which could allow an attacker to take complete control of an affected system. Adobe Shockwave is a multimedia platform used to add animation and interactivity to web pages. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page or when a user opens a specially crafted file. 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.

SYSTEMS AFFECTED:

- Adobe Shockwave Player (versions prior to 11.6.4.634)

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 Shockwave Player is prone to five memory corruption vulnerabilities that could allow for remote code execution.

Successful exploitation of any of these vulnerabilities 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:

Update to Adobe Shockwave Player 11.6.5.635 immediately after appropriate testing.

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 un-trusted websites or follow links provided by unknown or un-trusted sources.

Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

Consider implementing file extension white lists for allowed e-mail attachments.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb12-13.html>

Security Focus:

<http://www.securityfocus.com/bid/53420>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2029>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2030>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2031>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2032>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2033>