

*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:**

10/28/2010

**SUBJECT:**

Multiple Vulnerabilities in Adobe Shockwave Player Could Allow Remote Code Execution

**OVERVIEW:**

Adobe has provided an update that addresses multiple vulnerabilities in Adobe Shockwave Player. These vulnerabilities could allow an attacker to take complete control of an affected system. Adobe Shockwave Player is a prevalent multimedia application used to display animations and video. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page. Exploitation may also occur when a user opens a specially crafted Shockwave (SWF) file. Successful exploitation will 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.

**Adobe is reporting that some of these vulnerabilities are being exploited on the Internet.**

**SYSTEMS AFFECTED:**

Adobe Shockwave Player 11.5.8.612 and earlier

**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 has provided an update that addresses eleven security vulnerabilities in Adobe Shockwave Player. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page. Exploitation may also occur when a user opens a specially crafted Shockwave (SWF) file.

There are 9 memory corruption vulnerabilities that could result in remote code execution.

A heap-based buffer overflow vulnerability may result in remote code execution.

A stack overflow vulnerability in the dirapi.dll module that could lead to code execution

**Adobe is reporting that some of these vulnerabilities are being exploited on the Internet.**

Successful exploitation of the remote code execution vulnerabilities will 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.

**RECOMMENDATIONS:**

The following actions should be taken:

- Systems running Adobe Shockwave Player 11.5.8.612 and earlier versions should be updated to version 11.5.9.615 immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Do not open email attachments from unknown or un-trusted sources.

**REFERENCES:**

**Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb10-25.html>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3653>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2581>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2582>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3655>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4084>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4085>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4086>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4087>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4088>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4089>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4090>

**Security Focus:**

<http://www.securityfocus.com/bid/44521>

<http://www.securityfocus.com/bid/44514>

<http://www.securityfocus.com/bid/44515>

<http://www.securityfocus.com/bid/44518>

<http://www.securityfocus.com/bid/44519>

<http://www.securityfocus.com/bid/44520>

<http://www.securityfocus.com/bid/44517>

<http://www.securityfocus.com/bid/44516>

<http://www.securityfocus.com/bid/44513>

<http://www.securityfocus.com/bid/44512>