

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:

6/11/2010

SUBJECT:

Multiple Vulnerabilities Discovered in Adobe Products

OVERVIEW:

Thirty vulnerabilities have been discovered in Adobe Flash Player and Adobe AIR. Adobe Flash Player is a widely distributed multimedia and application player for Microsoft Windows, Mozilla, and Apple systems. It is used to enhance the user experience when visiting web pages or reading email messages. Adobe AIR is a cross-platform runtime for developing Internet applications on the desktop. These vulnerabilities can be exploited if a user visits a malicious website or opens an email attachment containing Flash media designed to exploit these vulnerabilities.

Successful exploitation of twenty seven 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, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. The remaining vulnerabilities could allow an attacker to direct malicious content to a web browser or create denial of service conditions.

SYSTEMS AFFECTED:

Adobe Flash Player 10.0.45.2 and earlier
Adobe AIR 1.5.3.9130 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:

Thirty security vulnerabilities have been identified in Adobe Flash Player and Adobe AIR. These vulnerabilities can be exploited if a user visits a malicious website or opens an email attachment containing a Flash media file designed to trigger these issues. The vulnerabilities are as follows:

Fourteen vulnerabilities caused by unspecified Memory Corruption errors could result in remote code-execution.

Multiple heap-based buffer-overflow vulnerabilities could result in remote arbitrary code-execution.

Three integer-overflow vulnerabilities could result in remote code-execution.

Two invalid-pointer vulnerabilities could result in remote arbitrary code-execution.

A remote code-execution vulnerability caused by an indexing issue.

A remote arbitrary code-execution vulnerability caused by a memory-exhaustion issue.
An unspecified buffer-overflow vulnerability resulting in remote code-execution.
A remote arbitrary code-execution vulnerability due to a user-after-free condition.
A heap-corruption vulnerability could result in remote arbitrary code-execution.
A remote code-execution vulnerability due to a pointer memory-corruption issue.
A denial-of-service vulnerability affecting Flash Player 9 on unspecified UNIX platforms.
A denial-of-service vulnerability affecting unspecified vectors. Remote code-execution has not been ruled out.
A URL parsing vulnerability could lead to cross-site scripting attacks and is exploited only through Firefox and Chrome web browsers.

Successful exploitation of these vulnerabilities could allow an attacker to gain 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:

- Apply appropriate updates provided by Adobe to vulnerable systems immediately after appropriate testing.
- Systems running Adobe Flash Player 10.0.45.2 and earlier versions should be updated to version 10.1.53.64. Please note that according to KrebsSecurity, if you use both Internet Explorer and non-IE browsers, you're going to need to apply this update twice, once by visiting the [Flash Player installation page](#) with IE and then again with Firefox, Opera, or whatever other browser you use.
- Systems running Adobe AIR 1.5.3.9130 and earlier versions should be updated to version 2.0.2.12610.
- Do not open email attachments from unknown or un-trusted sources.
- Do not 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.

REFERENCES:

Security Focus:

(Please note that clicking on this link which includes Proof Of Concept code may create a false positive alert by your AV program)

<http://www.securityfocus.com/bid/40759>

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb10-14.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3793>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2160>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2161>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2162>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2163>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2164>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2165>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2166>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2167>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2169>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2170>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2171>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2172>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2173>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2174>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2175>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2176>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2177>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2178>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2179>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2180>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2181>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2182>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2183>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2184>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2185>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2186>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2187>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2188>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2189>

iDefense Labs:

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=871>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=872>

KrebsonSecurity

<http://krebsonsecurity.com/>