

EOC Information Alert

02/09/2011

DATE(S) ISSUED:

2/9/2011

SUBJECT:

Multiple Vulnerabilities in Adobe Shockwave

OVERVIEW:

Twenty-one 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 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. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:

Adobe Shockwave 11.5.9.615 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:

Twenty-one security vulnerabilities have been identified in Adobe Shockwave. These vulnerabilities can be exploited if a user visits a malicious website or opens an email attachment containing a file designed to trigger these issues. The vulnerabilities are as follows:

Thirteen memory corruption vulnerabilities

Four input validation vulnerabilities

One use-after-free vulnerability

Two integer overflow vulnerabilities

One buffer overflow vulnerability

Successful exploitation of any of these vulnerabilities may result in an attacker gaining the same user 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.

RECOMMENDATIONS:

We recommend the following actions be taken:

Apply the appropriate updates provided by Adobe immediately after appropriate testing.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

Remind users not to open email attachments from unknown or un-trusted sources.

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

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb11-01.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2587>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2588>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2589>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4092>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4093>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4187>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4188>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4189>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4190>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4191>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4192>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4193>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4194>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4195>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4196>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4306>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4307>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0555>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0556>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0557>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0569>

EOC
490 18th Street
Helena, MT 59601
24x7 Operations Line (406) 444-2000
1-800-628-4917