

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:

03/28/2012

04/05/2012 - UPDATED

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB12-07)

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 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.

SYSTEMS AFFECTED:

- Adobe Flash Player 11.1.102.63 and earlier for Windows, Macintosh, Linux, and Solaris
- Adobe Flash Player 11.1.111.7 for Android versions 3.x and 2.x
- Adobe AIR 3.1.0.4880 and earlier versions for Windows, Macintosh, and Android

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

ORIGINAL DESCRIPTION:

Adobe Flash Player is prone to two unspecified memory corruption vulnerabilities which could allow for remote code execution.

- An unspecified memory corruption vulnerability exists due to the way the application handles URL security domain checking. (CVE-2012-0772)
- An unspecified memory corruption vulnerability exists in the application's NetStream class. (CVE-2012-0773)

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 result in denial-of-service conditions.

April 5 - UPDATED DESCRIPTION:

Two Flash Player memory corruption vulnerabilities have been reported in the Chrome interface (Google Chrome only) (CVE-2012-0724, CVE-2012-0725). The Google Chrome version 18.0.1025.151 update addresses these vulnerabilities.

RECOMMENDATIONS:

The following actions should be taken:

- Install the update from 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 from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

ORIGINAL REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb12-07.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0772>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0773>

Security Focus

<http://www.securityfocus.com/bid/52748>

April 5 - UPDATED REFERENCES:

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0724>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0725>