

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:

08/10/2011

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB11-21)

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 10.3.181.36 and earlier versions for Windows, Macintosh, Linux, and Solaris operating systems
- Adobe Flash Player 10.3.185.25 and earlier versions for Android
- Adobe AIR 2.7 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**

DESCRIPTION:

Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution.

Details of these vulnerabilities are as follows:

- One cross-site information disclosure vulnerability
- Three integer overflow vulnerabilities
- Four memory corruption vulnerabilities
- Five bounds checking vulnerabilities

All of these vulnerabilities may be exploited if a user opens a specially crafted Adobe Flash file or visits a specially crafted webpage, which may be sent via email. 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.

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 or click on URLs from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb11-21.html>

SecurityFocus:

<http://www.securityfocus.com/bid/49073>

<http://www.securityfocus.com/bid/49074>

<http://www.securityfocus.com/bid/49075>

<http://www.securityfocus.com/bid/49076>

<http://www.securityfocus.com/bid/49077>

<http://www.securityfocus.com/bid/49079>

<http://www.securityfocus.com/bid/49080>

<http://www.securityfocus.com/bid/49081>

<http://www.securityfocus.com/bid/49082>

<http://www.securityfocus.com/bid/49083>

<http://www.securityfocus.com/bid/49084>

<http://www.securityfocus.com/bid/49085>

<http://www.securityfocus.com/bid/49086>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2130>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2134>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2135>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2136>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2137>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2138>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2139>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2140>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2414>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2415>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2416>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2417>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2425>