

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:

2/16/2012

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB12-03)

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 result in denial-of-service conditions.

Please note that Adobe is acknowledging active exploitation of the cross-site scripting vulnerability. These attacks have been targeted to users via a malicious link to delivered in an e-mail.

SYSTEMS AFFECTED:

- Flash Player 11.1.102.55 and earlier
- Flash Player 11.1.112.61 and earlier for Android 4.x
- Flash Player 11.1.111.5 and earlier for Android 3.x and 2.x
- Flash Player 11.1.102.55 and earlier for Chrome users

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 memory corruption vulnerabilities, security bypass vulnerabilities and a cross-site scripting vulnerability which could allow for remote code execution. Details of these vulnerabilities are as follows:

- Multiple unspecified memory corruption vulnerabilities exist in Flash which could lead to remote code execution.
- A type confusion memory corruption vulnerability that could lead to code execution.
- An MP4 parsing memory corruption vulnerability that could lead to code execution

- Two security bypass vulnerabilities that could lead to code execution
- An Active-X cross-site scripting vulnerability exists that could be used to take actions on a user's behalf on any website or webmail provider. This issue only affects Internet Explorer on Microsoft Windows.

To exploit these vulnerabilities an attacker must create a specially crafted file or URL and distributes that file or URL to unsuspecting users via e-mail or some other means. When the file or URL is executed, the exploit occurs.

Please note that Adobe is acknowledging active exploitation of the cross-site scripting vulnerability. These attacks have been targeted to users via a malicious link to delivered in an e-mail.

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.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the updates provided by 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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb12-03.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0751>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0752>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0753>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0754>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0755>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0756>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0767>

Security Focus:

<http://www.securityfocus.com/bid/52037>

<http://www.securityfocus.com/bid/52032>

<http://www.securityfocus.com/bid/52033>

<http://www.securityfocus.com/bid/52034>

<http://www.securityfocus.com/bid/52035>

<http://www.securityfocus.com/bid/52036>

<http://www.securityfocus.com/bid/52040>