

*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:**

**4/12/2011**

**SUBJECT:**

New Vulnerability in Adobe Flash Player Could Allow For Remote Code Execution

**OVERVIEW:**

A vulnerability has been discovered in Adobe Flash Player which 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. This vulnerability may be exploited if a user opens a Microsoft Word document containing an embedded specially crafted Adobe Flash file, which may be sent as an email attachment. Successful exploitation will cause the application to crash and could also 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.

There are reports of active exploitation of this vulnerability.

Adobe Reader 9.x for UNIX, Adobe Reader for Android, and Adobe Reader and Acrobat 8.x are not affected by this issue.

**SYSTEMS AFFECTED:**

Adobe Flash Player 10.2.153.1 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems.  
Adobe Flash Player 10.2.154.25 and earlier for Chrome users.  
Adobe Flash Player 10.2.156.12 and earlier for Android.  
The Authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.2) and earlier 10.x and 9.x versions for Windows and Macintosh operating systems.

**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 a vulnerability that allows for remote code execution. Successful exploitation of this vulnerability 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. There have been reports indicating active exploitation of this vulnerability due to opening a Microsoft Word (.doc) file sent as an email attachment and embedded with a specially crafted Flash (.swf) file. Users should assume this vulnerability could be exploited in any rich content capable file format at this time.

Adobe is reporting that this vulnerability may also impact the authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.2) and earlier 10.x and 9.x versions for Windows and Macintosh operating systems. However, Adobe is not currently aware of attacks targeting Adobe Reader and Acrobat when opening PDF files. Adobe Reader X with Protected Mode enabled would prevent an exploit of this kind from executing.

There are reports of active exploitation of this vulnerability.

Adobe Reader 9.x for UNIX, Adobe Reader for Android, and Adobe Reader and Acrobat 8.x are not affected by this issue.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Install the patch/update from Adobe as soon as it becomes available after appropriate testing.

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

- Consider installing and running Adobe Reader X in Protected Mode.

- Do not open email attachments from unknown or un-trusted sources.

- Consider implementing file extension whitelists for allowed e-mail attachments.

#### **REFERENCES:**

##### **Adobe:**

<http://www.adobe.com/support/security/advisories/apsa11-02.html>

##### **SecurityFocus:**

<http://www.securityfocus.com/bid/47314>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0611>