

ISSO Information Alert

03/22/2011

MS-ISAC ADVISORY NUMBER:

2011-015 - *UPDATED*

DATE(S) ISSUED:

3/14/2011

3/22/2011 - Updated

SUBJECT:

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

ORIGINAL OVERVIEW:

A new vulnerability has been discovered in the 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 when a user opens a Microsoft Excel file embedded with a specially crafted Adobe Flash file, which is 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.

UPDATED OVERVIEW:

Adobe has released an update that resolves the reported vulnerabilities for Flash, Adobe Reader and Adobe Acrobat. Please note that this vulnerability has not been fixed in Adobe Reader X for Windows. Adobe plans to release an update for Adobe Reader X during the next quarterly security update on June 14, 2011.

SYSTEMS AFFECTED:

- Adobe Flash Player 10.2.152.33 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems.
- Adobe Flash Player 10.2.154.13 and earlier for Chrome users.
- Adobe Flash Player 10.1.106.16 and earlier for Android.
- The Authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.1) 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

ORIGINAL DESCRIPTION:

Adobe Flash is prone to a vulnerability that will cause the application to crash when opening a Microsoft Excel (.xls) file sent as an email attachment and embedded with a specially crafted Flash (.swf) file.

Successful exploitation 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.

Adobe is reporting that this vulnerability may also impact the authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.1) 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. 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.

UPDATED DESCRIPTION:

Adobe has released an update that resolves the reported vulnerabilities for Flash, Adobe Reader and Adobe Acrobat. Please note that this vulnerability has not been fixed in Adobe Reader X for Windows. Adobe plans to release an update for Adobe Reader X during the next quarterly security update on June 14, 2011.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions 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.

UPDATED RECOMMENDATIONS:

We recommend the following actions be taken:

- *Apply appropriate updates provided by Adobe to vulnerable systems immediately after appropriate testing.*

ORIGINAL REFERENCES:**Adobe:**

<http://www.adobe.com/support/security/advisories/apsa11-01.html>

SecurityFocus:

<http://www.securityfocus.com/bid/46860>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0609>

UPDATED REFERENCES:**Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb11-05.html>

<http://www.adobe.com/support/security/bulletins/apsb11-06.html>