Security bulletin

Security updates available for Adobe Reader and Acrobat

Release date: February 20, 2013

Vulnerability identifier: APSB13-07

Priority: See table below

CVE number: CVE-2013-0640, CVE-2013-0641

Platform: All Platforms

SUMMARY

Adobe has released security updates for Adobe Reader and Acrobat XI (11.0.01 and earlier) for Windows and Macintosh, X (10.1.5 and earlier) for Windows and Macintosh, 9.5.3 and earlier 9.x versions for Windows and Macintosh, and Adobe Reader 9.5.3 and earlier 9.x versions for Linux. These updates address vulnerabilities that could cause a crash and potentially allow an attacker to take control of the affected system.

Adobe recommends users update their product installations to the latest versions:

- Users of Adobe Reader XI (11.0.01 and earlier) for Windows and Macintosh should update to Adobe Reader XI (11.0.02).
- For users of Adobe Reader X (10.1.5 and earlier) for Windows and Macintosh, who cannot update to Adobe Reader XI (11.0.02), Adobe has made available the update Adobe Reader X (10.1.6).
- For users of Adobe Reader 9.5.3 and earlier 9.x versions for Windows and Macintosh, who cannot update to Adobe Reader XI (11.0.02), Adobe has made available the update Adobe Reader 9.5.4.
- Users of Adobe Reader 9.5.3 and earlier 9.x versions for Linux should update to Adobe Reader 9.5.4.
- Users of Adobe Acrobat XI (11.0.01 and earlier) for Windows and Macintosh should update to Adobe Acrobat XI (11.0.02).
- Users of Adobe Acrobat X (10.1.5 and earlier) for Windows and Macintosh should update to Adobe Acrobat X (10.1.6).
- Users of Adobe Acrobat 9.5.3 and earlier 9.x versions for Windows and Macintosh should update to Adobe Acrobat 9.5.4.

Adobe is aware of reports that two vulnerabilities (CVE-2013-0640, CVE-2013-0641) referenced in Security Advisory APSA13-02 are being exploited in the wild. Adobe recommends users update their product installations using the instructions provided in the "Solution" section below.

AFFECTED SOFTWARE VERSIONS

- Adobe Reader XI (11.0.01 and earlier) for Windows and Macintosh
- Adobe Reader X (10.1.5 and earlier) for Windows and Macintosh
- Adobe Reader 9.5.3 and earlier 9.x versions for Windows, Macintosh and Linux
- Adobe Acrobat XI (11.0.01 and earlier) for Windows and Macintosh
- Adobe Acrobat X (10.1.5 and earlier) for Windows and Macintosh
- Adobe Acrobat 9.5.3 and earlier 9.x versions for Windows and Macintosh

SOLUTION

Adobe recommends users update their software installations by following the instructions below:

Adobe Reader

Users on Windows and Macintosh can utilize the product's update mechanism. The default configuration is set to run automatic update checks on a regular schedule. Update checks can be manually activated by choosing Help > Check for Updates.

Adobe Reader users on Windows can also find the appropriate update here:
http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows

Adobe Reader users on Macintosh can also find the appropriate update here:
http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh

Adobe Reader users on Linux can find the appropriate update here: ftp://ftp.adobe.com/pub/adobe/reader/unix/9.x/

Adobe Acrobat

Users can utilize the product's update mechanism. The default configuration is set to run automatic update checks on a regular schedule. Update checks can be manually activated by choosing Help > Check for Updates.

Acrobat Standard, Pro and Pro Extended users on Windows can also find the appropriate update here:
http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Windows

Acrobat Pro users on Macintosh can also find the appropriate update here:

http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Macintosh

PRIORITY AND SEVERITY RATINGS

Adobe categorizes these updates with the following priority ratings and recommends users update their installations to the newest versions:

Product	Updated version	Platform	Priority rating
Adobe Reader	XI (11.0.02)	Windows and Macintosh	1
	X (10.1.6)	Windows and Macintosh	1
	9.5.4	Windows and Macintosh	1
	9.5.4	Linux	2
Adobe Acrobat	XI (11.0.02)	Windows and Macintosh	1
	X (10.1.6)	Windows and Macintosh	1
	9.5.4	Windows and Macintosh	1

These updates address critical vulnerabilities in the software.

DETAILS

Adobe has released security updates for Adobe Reader and Acrobat XI (11.0.01 and earlier) for Windows and Macintosh, X (10.1.5 and earlier) for Windows and Macintosh, 9.5.3 and earlier 9.x versions for Windows and Macintosh, and Adobe Reader 9.5.3 and earlier 9.x versions for Linux. These updates address vulnerabilities that could cause a crash and potentially allow an attacker to take control of the affected system.

Adobe recommends users update their product installations to the latest versions:

- Users of Adobe Reader XI (11.0.01 and earlier) for Windows and Macintosh should update to Adobe Reader XI (11.0.02).
- For users of Adobe Reader X (10.1.5 and earlier) for Windows and Macintosh, who cannot update to Adobe Reader XI (11.0.02), Adobe has made available the update Adobe Reader X (10.1.6).
- For users of Adobe Reader 9.5.3 and earlier 9.x versions for Windows and Macintosh, who cannot update to Adobe Reader XI (11.0.02), Adobe has made available the update Adobe Reader 9.5.4.
- Users of Adobe Reader 9.5.3 and earlier 9.x versions for Linux should update to Adobe Reader 9.5.4.
- Users of Adobe Acrobat XI (11.0.01 and earlier) for Windows and Macintosh should update to Adobe Acrobat XI (11.0.02).
- Users of Adobe Acrobat X (10.1.5 and earlier) for Windows and Macintosh should update to Adobe Acrobat X (10.1.6).
- Users of Adobe Acrobat 9.5.3 and earlier 9.x versions for Windows and Macintosh should update to Adobe Acrobat 9.5.4.

Adobe is aware of reports that two vulnerabilities (CVE-2013-0640, CVE-2013-0641) referenced in Security Advisory APSA13-02 are being exploited in the wild. Adobe recommends users update their product installations using the instructions provided in the "Solution" section above.

These updates resolve a memory corruption vulnerability that could lead to code execution (CVE-2013-0640).

These updates resolve a buffer overflow vulnerability that could lead to code execution (CVE-2013-0641).

Products
- Adobe Creative Cloud
- Creative Suite 6
- Adobe Marketing Cloud
- Acrobat
- Photoshop
- Digital Publishing Suite
- Elements family
- SiteCatalyst
- For education

Download
- Product trials
- Adobe Reader
- Adobe Flash Player
- Adobe AIR

Support & Learning
- Product help
- Forums

Buy
- For personal and professional use
- For students, educators, and staff
- For small and medium businesses
- Volume Licensing
- Special offers

Company
- News room
- Partner programs
- Corporate responsibility
- Career opportunities
- Investor Relations
- Events
- Legal
- Security
- Contact Adobe

Choose your region