Robert Babezki

From: US-CERT Technical Alerts [technical-alerts@us-cert.gov]
Sent: Friday, February 20, 2009 4:06 PM
To: technical-alerts@us-cert.gov
Subject: US-CERT Technical Cyber Security Alert TA09-051A -- Adobe Acrobat and Reader Vulnerability

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

National Cyber Alert System

Technical Cyber Security Alert TA09-051A

Adobe Acrobat and Reader Vulnerability

Original release date: February 20, 2009
Last revised: --
Source: US-CERT

Systems Affected

* Adobe Reader version 9 and earlier
* Adobe Acrobat (Professional, 3D, and Standard) version 9 and earlier

Overview

Adobe has released Security Bulletin APSB09-01, which describes a vulnerability that affects Adobe Reader and Acrobat. This vulnerability could allow a remote attacker to execute arbitrary code.

I. Description

Adobe Security Bulletin APSB09-01 describes a memory-corruption vulnerability that affects Adobe Reader and Acrobat. Further details are available in Vulnerability Note VU#905281. An attacker could exploit these vulnerabilities by convincing a user to load a specially crafted Adobe Portable Document Format (PDF) file. Acrobat integrates with popular web browsers, and visiting a website is usually sufficient to cause Acrobat to load PDF content.

II. Impact

An attacker may be able to execute arbitrary code.

III. Solution

Disable JavaScript in Adobe Reader and Acrobat

Disabling Javascript may prevent some exploits from resulting in code execution. Acrobat JavaScript can be disabled using the Preferences menu (Edit -> Preferences -> JavaScript and un-check Enable Acrobat JavaScript).

Prevent Internet Explorer from automatically opening PDF documents

The installer for Adobe Reader and Acrobat configures Internet Explorer to automatically open PDF files without any user interaction. This behavior can be reverted to the safer option of prompting the user by importing the following as a .REG file:

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\AcroExch.Document.7]
"EditFlags"=hex:00,00,00,00
```

Disable the display of PDF documents in the web browser

Preventing PDF documents from opening inside a web browser will partially mitigate this vulnerability. If this workaround is applied it may also mitigate future vulnerabilities. To prevent PDF documents from automatically being opened in a web browser, do the following:

1. Open Adobe Acrobat Reader.
2. Open the Edit menu.
3. Choose the preferences option.
4. Choose the Internet section.
5. Un-check the "Display PDF in browser" check box.

Do not access PDF documents from untrusted sources

Do not open unfamiliar or unexpected PDF documents, particularly those hosted on web sites or delivered as email attachments. Please see Cyber Security Tip ST04-010.

IV. References

* Adobe Security Bulletin apsa09-01 - <http://www.adobe.com/support/security/advisories/apsa09-01.html>

* Securing Your Web Browser - <http://www.us-cert.gov/reading_room/securing_browser/>

* Vulnerability Note VU#905281 - <http://www.kb.cert.org/vuls/id/905281>

The most recent version of this document can be found at:

<http://www.us-cert.gov/cas/techalerts/TA09-051A.html>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@cert.org> with "TA09-051A Feedback VU#905281" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <http://www.us-cert.gov/cas/signup.html>.

<http://www.us-cert.gov/legal.html>

Revision History

February 20, 2009: Initial release

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.5 (GNU/Linux)

iQEVAwUBSZ8ayXIHljM+H4irAQIUcAf+M01pEVt0f1ZdRvCQwSYw1efnHu4YGdhI
xT27jeKvaW/h6ghGx0L9YWCSn/A2LY3D+fDU1PZmWi7TT/SMEQ8LvKomyCu026Dv
fD63qIXYj3NoPu11bINKFX4HFQCOYWKuM/58Y8mDQXOg0RLhePfMhMbB/S5/xpNT
J09FupEgMvbD+tjVILP+W8JSY4YtAxUJLHfB7cTTHGtlKZyAsnnmJM3Oi4au10DW
vqZD8JefoMLeV2MTGRyP4HGTaRxVY1+yucXO1KBGnKX7otCRkCWOupEuKw+tIEkT
YsYIlkH5MzftkesSEDpDMIAiIE+uprJRv2HGkc38Rhbs/03JyxxVlA==
=HSro
-----END PGP SIGNATURE-----