

[NT] Adobe Reader and Acrobat JavaScript Insecure Method Exposure Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00028.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 10 Feb 2008 19:33:08 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Adobe Reader and Acrobat JavaScript Insecure Method Exposure Vulnerability

SUMMARY

<<http://www.adobe.com/products/acrobat/>> Adobe Reader is "a program for viewing Portable Document Format (PDF) documents. Acrobat is the program used to create such documents". Remote exploitation of an insecure method exposed by the JavaScript library in Adobe Reader and Acrobat could allow an attacker to execute arbitrary code as the current user.

DETAILS

Vulnerable Systems:

- * Adobe Reader version 8.1 on Windows XP SP2

Immune Systems:

- * Adobe Reader version 8.1.2

Adobe Reader and Acrobat implement a version of JavaScript in the EScript.api plug-in which is based on the reference implementation used in Mozilla products. One of the methods exposed allows direct control over low level features of the object, which in turn allows execution of arbitrary code.

[NT] Adobe Reader and Acrobat JavaScript Insecure Method Exposure Vulnerability

Analysis:

Exploitation of this vulnerability would allow an attacker to execute arbitrary code as the current user. In order to exploit this vulnerability, an attacker would have to convince the targeted user to open a maliciously constructed file. This file could be sent directly to the targeted user or linked from a website.

Insufficient error checking is performed on the input which allows, among other things, attacker-supplied data to be written to arbitrary offsets in memory, potentially resulting in arbitrary code execution.

Workaround:

Disabling JavaScript in Adobe Reader or Acrobat will limit exposure to this vulnerability. When JavaScript is disabled, Adobe Reader will prompt the user that some components of the document may not function, and provide an opportunity to enable it.

Vendor response:

Adobe released version 8.1.2 of Adobe Reader and Acrobat to address this vulnerability. Although there is currently no update for version 7.0.9, Adobe reports it does plan to release one at a later date. For more information, visit the vendor's advisory at the following URL:

<<http://www.adobe.com/support/security/advisories/apsa08-01.html>>
<http://www.adobe.com/support/security/advisories/apsa08-01.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5663>>
CVE-2007-5663

Disclosure timeline:

10/03/2007 – Initial vendor notification
10/03/2007 – Initial vendor response
10/26/2007 – Request for status
10/26/2007 – Status – Est. early January
01/04/2008 – Request for status
01/04/2008 – Status – Scheduled early February
01/28/2008 – Adobe plans patch for 8, but not 7
01/30/2008 – Concerns about the plan e-mailed to Adobe
01/31/2008 – Telephone call to clarify concerns
02/06/2008 – Adobe releases 8.1.2
02/07/2008 – Adobe publishes APSA08-01
02/08/2008 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=656>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=656>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.