

[NT] Adobe Acrobat/Reader 6 Local Files Access

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0053.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/13/04

To: list@securiteam.com

Date: 13 Oct 2004 18:57:18 +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 Acrobat/Reader 6 Local Files Access

SUMMARY

Acrobat/ Acrobat reader is software for viewing and printing Adobe Portable Document Format (PDF) files. Adobe PDF files can be viewed on most major operating systems.

Version 6 of this program has an issue with the way it handles embedding macromedia flash files directly into a pdf. This allows a malicious website operator to steal local files from a user's hard drive including cookie files.

DETAILS

Vulnerable Systems:

- * Adobe Reader version 6.0.1
- * Adobe Acrobat version 6

Version 6 of the pdf format introduced a new way to embed movies directly into the pdf file. In previous versions one could only link to media in external files

Adobe reader extracts this swf file from the pdf and saves it under a random name to your temp dir, on windows XP and 2000 this dir is usually

Securiteam: [NT] Adobe Acrobat/Reader 6 Local Files Access

located at: C:\Documents and Settings\\Local Settings\Temp

It then appears to "link" directly to this saved file in effect making your local hard disk the codebase for this swf file and allowing it read access to all of the files on your hard drive

Demonstration:

Create a text file called c:\jelmer.txt then proceed to click on:

<http://62.131.86.111/security/acrobat/demo.pdf>

ADDITIONAL INFORMATION

The information has been provided by <mailto:jkuperus@planet.nl> Jelmer.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.