

Adobe acrobat / Adobe Reader 6 can read local files

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-10/0119.html>

From: Jelmer (*jkuperus_at_planet.nl*)

Date: 10/12/04

Date: Tue, 12 Oct 2004 15:56:32 +0200

To: bugtraq@securityfocus.com, full-disclosure@lists.netsys.com

Adobe acrobat / Adobe Reader 6 can read local files

Description

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

Technical Details:

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 located at

C:\Documents and Settings\<<username>\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

Systems affected:

Adobe reader 6
Adobe acrobat 6

Demonstration:

SecurityFocus Bugtraq: Adobe acrobat / Adobe Reader 6 can read local files

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

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

Risk: medium