

Full-Disclosure: RE: [Full-Disclosure] Re: Adobe acrobat / Adobe Reader 6 can read local files

## RE: [Full-Disclosure] Re: Adobe acrobat / Adobe Reader 6 can read local files

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/0400.html>

---

**From:** Jelmer (*jkuperus\_at\_planet.nl*)

**Date:** 10/13/04

To: "'Jay Libove'" <libove@felines.org>, full-disclosure@lists.netsys.com

Date: Wed, 13 Oct 2004 02:28:39 +0200

The demo uses script behind the scenes to start the movie, So the demo would fail if you disabled scripting

I don't believe there's a way to start the movie without with scripting disabled. So you should be safe. But I'll admit to being anything but an expert on pdf.. Yet anyway so I might me overlooking something

—jelmer

-----Original Message-----

From: full-disclosure-admin@lists.netsys.com

[mailto:full-disclosure-admin@lists.netsys.com] On Behalf Of Jay Libove

Sent: dinsdag 12 oktober 2004 19:01

To: full-disclosure@lists.netsys.com

Subject: [Full-Disclosure] Re: Adobe acrobat / Adobe Reader 6 can read local files

I have Acrobat Reader configured to NOT run Javascript. The demo did not work on my system (XP, SP2, Acrobat Reader v6.0.2 dated 5/18/2004).

So, is having JavaScript enabled also a requirement in order for this embedded SWF exploit to work?

—Jay Libove, CISSP

> *Message:* 20

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

> *From:* Jelmer <jkuperus@planet.nl>

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

> *Subject:* [Full-Disclosure] Adobe acrobat / Adobe Reader 6 can read local files

>

> *Adobe acrobat / Adobe Reader 6 can read local files*

>

> *Description*

RE: [Full-Disclosure] Re: Adobe acrobat / Adobe Reader 6 can read local files

Full-Disclosure: RE: [Full-Disclosure] Re: Adobe acrobat / Adobe Reader 6 can read local files

- >
- > *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\\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:*
- >
- > *Create a text file called c:\jelmer.txt then proceed to click on*
- >
- > *<http://62.131.86.111/security/acrobat/demo.pdf>*
- >
- > *Risk: medium*

---

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

---

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

RE: [Full-Disclosure] Re: Adobe acrobat / Adobe Reader 6 can read local files