

# [UNIX] Insecure Temporary Files in Acrobat Reader

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0097.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 06/21/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Fri, 21 Jun 2002 07:43:07 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Insecure Temporary Files in Acrobat Reader

---

## SUMMARY

Acrobat Reader (acroread) has been found to create temporary files in /tmp (or in directory pointed by TMP environment variable) insecurely when it opens or prints a PDF document. The vulnerability would allow the use of a symbolic link to cause the overwriting of system sensitive files.

## DETAILS

Vulnerable systems:

- \* Acrobat Reader version 5.04 and prior (UNIX)

Immune systems:

- \* Acrobat Reader version 5.05 (UNIX)

By straced "acroread" you can monitor the way it handles file and more specifically temporary files. From the strace output you should notice that "acroread" opens up temporary files in /tmp (or in \$TMP if you have it set) without using O\_EXCL, therefore "acroread" will follow symbolic links when it creates a temporary file.

Here is an example (gathered from a strace output) that shows the problem:

```
stat("/tmp/Acro48IBR1", 0xbfffe958) = -1 ENOENT (No such file or directory)
```

## Securiteam: [UNIX] Insecure Temporary Files in Acrobat Reader

```
open("/tmp/Acro48IBR1", O_RDWR|O_CREAT|O_TRUNC, 0666) = 5
...
...
unlink("/tmp/Acro48IBR1") = 0
```

These temporary files were created while the program was opening a document and printing a document (Print To: Printer Command).

### Workaround:

Set TMP environment variable to a secure directory (e.g. ~/tmp) before using Acrobat Reader (and possibly before launching Netscape if you use the acrobat plugin). One possible way to achieve this would be to replace the acroread shell script with a script that sets TMP and then execs the original acroread (or directly modify the acroread script if the license permits this).

### Solution:

Acrobat Reader 5.05 appears to correct this problem. Download the updated version from: <http://www.adobe.com>

### Vendor status:

[security@adobe.com](mailto:security@adobe.com) Adobe contacted on Thu 19 Jul 2001. Adobe said that they'll look into this. Acrobat Reader 5.05 appears to correct the problem.

### ADDITIONAL INFORMATION

The information has been provided by [Jarno.Huuskonen@iki.fi](mailto:Jarno.Huuskonen@iki.fi)  
Jarno Huuskonen.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Xitami Web Server Plaintext Administrator Password Storage"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)