

# [UNIX] Xpdf Stream.cc Multiple Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-11/msg00019.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 8 Nov 2007 12:03:40 +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>

-----

Xpdf Stream.cc Multiple Vulnerabilities

---

## SUMMARY

<<http://www.foolabs.com/xpdf/>> Xpdf is "an open source viewer for Portable Document Format (PDF) files. (These are also sometimes also called 'Acrobat' files, from the name of Adobe's PDF software.) The Xpdf project also includes a PDF text extractor, PDF-to-PostScript converter, and various other utilities." Secunia Research has discovered some vulnerabilities in Xpdf, which can be exploited by malicious people to compromise a user's system.

## DETAILS

Vulnerable Systems:

\* Xpdf version 3.02 with xpdf-3.02p11.patch

1) An array indexing error within the "DCTStream::readProgressiveDataUnit()" method in xpdf/Stream.cc can be exploited to corrupt memory via a specially crafted PDF file.

2) An integer overflow error within the "DCTStream::reset()" method in xpdf/Stream.cc can be exploited to cause a heap-based buffer overflow via a specially crafted PDF file.

## [UNIX] Xpdf Stream.cc Multiple Vulnerabilities

3) A boundary error within the "CCITTFaxStream::lookChar()" method in xpdf/Stream.cc can be exploited to cause a heap-based buffer overflow by tricking a user into opening a PDF file containing a specially crafted "CCITTFaxDecode" filter.

Successful exploitation may allow execution of arbitrary code.

### Time Table:

17/10/2007 – Vendor notified.  
22/10/2007 – vendor-sec notified.  
19/10/2007 – Vendor response.  
07/11/2007 – Public disclosure.

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4352>>  
CVE-2007-4352,  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5392>>  
CVE-2007-5392 and  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5393>>  
CVE-2007-5393

### ADDITIONAL INFORMATION

The information has been provided by Secunia Research.

The original article can be found at:

<[http://secunia.com/secunia\\_research/2007-88/](http://secunia.com/secunia_research/2007-88/)>  
[http://secunia.com/secunia\\_research/2007-88/](http://secunia.com/secunia_research/2007-88/)

=====  
  
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.