

# [UNIX] Kpdf/Koffice Multiple Buffer Overflows (Xpdf)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00098.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 28 Dec 2005 12:16:06 +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>

-----

Kpdf/Koffice Multiple Buffer Overflows (Xpdf)

---

## SUMMARY

kpdf, the KDE pdf viewer, shares code with xpdf. xpdf contains multiple integer overflow vulnerabilities that allow specially crafted PDF files, when opened, to overflow a heap allocated buffer and execute arbitrary code.

A remotely supplied PDF files can be used to execute arbitrary code on the client machine if the user has decided to open it using kpdf.

## DETAILS

### Vulnerable Systems:

- \* KDE 3.2.0 up to including KDE 3.5.0
- \* KOffice 1.3.0 up to including KOffice 1.4.2

### Solution:

Source code patches have been made available which fix these vulnerabilities. Contact your OS vendor / binary package provider for information about how to obtain updated binary packages.

[UNIX] Kpdf/Koffice Multiple Buffer Overflows (Xpdf)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3191>>

CAN-2005-3191,

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3192>>

CAN-2005-3192,

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3193>>

CAN-2005-3193

Patch:

Patch for KDE 3.5.0 is available from

[ftp://ftp.kde.org/pub/kde/security\\_patches](ftp://ftp.kde.org/pub/kde/security_patches) :

04d1a115cca0deacbfca5c172bb9f4db

post-3.5.0-kdegraphics-CAN-2005-3193.diff

Patch for KDE 3.4.3 is available from

[ftp://ftp.kde.org/pub/kde/security\\_patches](ftp://ftp.kde.org/pub/kde/security_patches) :

b9787ff17e3e7eccee9ff23edcdca2c1

post-3.4.3-kdegraphics-CAN-2005-3193.diff

Patch for KDE 3.3.2 is available from

[ftp://ftp.kde.org/pub/kde/security\\_patches](ftp://ftp.kde.org/pub/kde/security_patches) :

8e0b2db76bc419b444f8308b3d8127b9

post-3.3.2-kdegraphics-CAN-2005-3193.diff

Patch for KDE 3.2.3 is available from

[ftp://ftp.kde.org/pub/kde/security\\_patches](ftp://ftp.kde.org/pub/kde/security_patches) :

657fb2de895e8945d8ba7d644ae10f6f

post-3.2.3-kdegraphics-CAN-2005-3193.diff

Patch for KOffice 1.3.0 and newer is available from

[ftp://ftp.kde.org/pub/kde/security\\_patches](ftp://ftp.kde.org/pub/kde/security_patches) :

f50a646d03bd33384c353195b9d298a0

post-1.3-koffice-CAN-2005-3193.diff

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.kde.org/info/security/advisory-20051207-1.txt>>

<http://www.kde.org/info/security/advisory-20051207-1.txt>

=====

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.

- 
- Prev by Date: [\*\[NEWS\] Portfolio Netpublish Server 'template' Directory Traversal\*](#)
  - Next by Date: [\*\[NEWS\] Symantec Antivirus RAR Library Multiple Heap Overflows\*](#)
  - Previous by thread: [\*\[NEWS\] Portfolio Netpublish Server 'template' Directory Traversal\*](#)
  - Next by thread: [\*\[NEWS\] Symantec Antivirus RAR Library Multiple Heap Overflows\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)