



CVE-2005-3627

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2005-3627
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-31 05:00:00 UTC
Updated	2018-10-19 15:37:00 UTC
Description	Stream.cc in Xpdf, as used in products such as gpdf, kpdf, pdftohtml, poppler, teTeX, CUPS, libextractor, and others, allows

Risk And Classification

Problem Types: CWE-119 | NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xpdf	Xpdf	All	All	All	All
Application	Xpdf	Xpdf	All	All	All	All

References

Reference	Source
Gentoo Linux Documentation -- Xpdf, Poppler, GPdf, libextractor, pdftohtml: Heap overflows	GENE
USN-236-1: xpdf vulnerabilities Ubuntu security notices	UBUN
Secunia - Advisories - Debian update for pdftkit.framework	SECU
[SECURITY] Fedora Core 3 Update: cups-1.1.22-0.rc1.8.9	CONI
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	SECU
Advisories - Mandriva Linux OS	MANI
[SECURITY] Fedora Core 4 Update: poppler-0.4.4-1.1	FEDC
Secunia - Advisories - Debian update for tetex-bin	SECU
Webmail - OVH	VUPE
Debian -- Security Information -- DSA-936-1 libextractor	DEBI
Webmail - OVH	VUPE
Secunia - Advisories - Mandriva update for cups	SECU

SecurityFocus	FEDC
Secunia - Advisories - Gentoo updates for xpdf/poppler/gpdf/libextractor/pdf-tohtml	SECU
Secunia - Advisories - Ubuntu updates for cupsys / libpoppler0c2 / tetex-bin / xpdf-reader / xpdf-utils	SECU
Debian -- Page not found	DEBI
Secunia - Advisories - xpdf Multiple Integer Overflow Vulnerabilities	SECU
Repository / Oval Repository	OVAL
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: xpdf,kpdf,gpdf,kword (SUSE-SA:2006:001)	SUSE
Debian -- Security Information -- DSA-962-1 pdf-tohtml	DEBI
Advisories - Mandriva Linux	MANI
rhn.redhat.com Red Hat Support	REDH
IBM X-Force Exchange	XF
Secunia - Advisories - Fedora update for cups	SECU
Secunia - Advisories - Slackware update for xpdf	SECU
Advisories - Mandriva Linux OS	MANI
20060201-01-U	SGI
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	SECU
20051201-01-U	SGI
Secunia - Advisories - Red Hat update for gpdf	SECU
Secunia - Advisories - teTeX Xpdf Multiple Integer Overflow Vulnerabilities	SECU
Secunia - Advisories - Fedora update for gpdf	SECU
20060101-01-U	SGI
Advisories - Mandriva Linux OS	MANI
Advisories - Mandriva Linux OS	MANI
Secunia - Advisories - Debian update for libextractor	SECU
Sun Solaris Gnome PDF Viewer Multiple Vulnerabilities - Advisories - Secunia	SECU
Debian -- Page not found	DEBI
Debian -- Page not found	DEBI
Gentoo Linux Documentation -- KPdf, KWord: Multiple overflows in included Xpdf code	GEN
Secunia - Advisories - Debian update for kpdf	SECU
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	SECU
[SECURITY] Fedora Core 4 Update: cups-1.1.23-15.3	CONI
Secunia - Advisories - Fedora update for poppler	SECU
Secunia - Advisories - Ubuntu update for kpdf / kword	SECU
The Slackware Linux Project: Slackware Security Advisories	SLAC
[SECURITY] Fedora Core 3 Update: gpdf-2.8.2-7.2	FEDC

KPDF and KWord Multiple Unspecified Buffer and Integer Overflow Vulnerabilities	BID
Debian -- Page not found	DEBI
Secunia - Advisories - Debian update for koffice	SECU
Secunia - Advisories - Gentoo update for kdegraphics / kpdf / koffice / kword	SECU
102972	SUN/
www.kde.org/info/security/advisory-20051207-2.txt	CONI
Debian -- Page not found	DEBI
rhn.redhat.com Red Hat Support	REDH
Advisories - Mandriva Linux OS	MANI
Advisories - Mandriva Linux OS	MANI
The Slackware Linux Project: Slackware Security Advisories	SLAC
Advisories - Mandriva Linux OS	MANI
Secunia - Advisories - libextractor Multiple Xpdf Vulnerabilities	SECU
Secunia - Advisories - SUSE updates for xpdf / kpdf / gpdf / kword	SECU
Secunia - Advisories - CUPS xpdf Multiple Integer Overflow Vulnerabilities	SECU
Secunia - Advisories - pdftohtml xpdf Multiple Integer Overflow Vulnerabilities	SECU
Secunia - Advisories - Debian update for pdftohtml	SECU
Debian -- Security Information -- DSA-961-1 pdfkit.framework	DEBI
Secunia - Advisories - Red Hat update for tetex	SECU
Secunia - Advisories - Debian update for cupsys	SECU
Secunia - Advisories - Slackware update for kdegraphics	SECU
Secunia - Advisories - Mandriva update for xpdf	SECU
Secunia - Advisories - GNUStep PDFKit Framework Xpdf Multiple Vulnerabilities	SECU
Secunia - Advisories - Debian update for xpdf	SECU
SCOSA-2006.15	SCO
SecurityFocus	FEDC
Secunia - Advisories - Red Hat update for cups	SECU
rhn.redhat.com Red Hat Support	REDH
Secunia - Advisories - Mandriva update for tetex	SECU
Debian -- Security Information -- DSA-950-1 cupsys	DEBI
Trustix update for multiple packages - Advisories - Secunia	SECU
scary.beasts.org/security/GESA-2005-003.txt	MISC
Secunia - Advisories - Poppler Xpdf Multiple Integer Overflow Vulnerabilities	SECU
Secunia - Advisories - Debian update for gpdf	SECU
2006-0002	TRUS
IBM X-Force Exchange	XF

Secunia - Advisories - Fedora update for tetex	SECU
SCO OpenServer update for xpdf - Advisories - Secunia	SECU
Secunia - Advisories - GNOME gpdf Xpdf Multiple Integer Overflow Vulnerabilities	SECU
CVE Program record	CVE.
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)