CVE-2005-3625

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2005-3625
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	Xpdf, as used in products such as gpdf, kpdf, pdftohtml, poppler, teTeX, CUPS, libextractor, and others, allows attackers to

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition
Operating System	Conectiva	Linux	10.0	All	All
Operating System	Conectiva	Linux	10.0	All	All
Operating System	Debian	Debian Linux	3.0	All	All
Operating System	Debian	Debian Linux	3.0	All	alpha
Operating System	Debian	Debian Linux	3.0	All	arm
Operating System	Debian	Debian Linux	3.0	All	hppa
Operating System	Debian	Debian Linux	3.0	All	ia-32
Operating System	Debian	Debian Linux	3.0	All	ia-64
Operating System	Debian	Debian Linux	3.0	All	m68k
Operating System	Debian	Debian Linux	3.0	All	mips
Operating System	Debian	Debian Linux	3.0	All	mipsel
Operating System	Debian	Debian Linux	3.0	All	ppc
Operating System	Debian	Debian Linux	3.0	All	s-390
Operating System	Debian	Debian Linux	3.0	All	sparc
Operating System	Debian	Debian Linux	3.1	All	All
Operating System	Debian	Debian Linux	3.1	All	alpha
Operating System	Debian	Debian Linux	3.1	All	amd64

Operating System	Debian	Debian Linux	3.1	All	arm
Operating System	Debian	Debian Linux	3.1	All	hppa
Operating System	Debian	Debian Linux	3.1	All	ia-32
Operating System	Debian	Debian Linux	3.1	All	ia-64
Operating System	Debian	Debian Linux	3.1	All	m68k
Operating System	Debian	Debian Linux	3.1	All	mips
Operating System	Debian	Debian Linux	3.1	All	mipsel
Operating System	Debian	Debian Linux	3.1	All	ppc
Operating System	Debian	Debian Linux	3.1	All	s-390
Operating System	Debian	Debian Linux	3.1	All	sparc
Operating System	Debian	Debian Linux	3.0	All	All
Operating System	Debian	Debian Linux	3.0	All	alpha
Operating System	Debian	Debian Linux	3.0	All	arm
Operating System	Debian	Debian Linux	3.0	All	hppa
Operating System	Debian	Debian Linux	3.0	All	ia-32
Operating System	Debian	Debian Linux	3.0	All	ia-64
Operating System	Debian	Debian Linux	3.0	All	m68k
Operating System	Debian	Debian Linux	3.0	All	mips
Operating System	Debian	Debian Linux	3.0	All	mipsel
Operating System	Debian	Debian Linux	3.0	All	ppc
Operating System	Debian	Debian Linux	3.0	All	s-390
Operating System	Debian	Debian Linux	3.0	All	sparc
Operating System	Debian	Debian Linux	3.1	All	All
Operating System	Debian	Debian Linux	3.1	All	alpha
Operating System	Debian	Debian Linux	3.1	All	amd64
Operating System	Debian	Debian Linux	3.1	All	arm
Operating System	Debian	Debian Linux	3.1	All	hppa
Operating System	Debian	Debian Linux	3.1	All	ia-32
Operating System	Debian	Debian Linux	3.1	All	ia-64
Operating System	Debian	Debian Linux	3.1	All	m68k
Operating System	Debian	Debian Linux	3.1	All	mips
Operating System	Debian	Debian Linux	3.1	All	mipsel
Operating System	Debian	Debian Linux	3.1	All	ppc
Operating System	Debian	Debian Linux	3.1	All	s-390
Operating System	Debian	Debian Linux	3.1	All	sparc

Application	Easy Software Products	Cups	1.1.22	All	All
Application	Easy Software Products	Cups	1.1.22_rc1	All	All
Application	Easy Software Products	Cups	1.1.23	All	All
Application	Easy Software Products	Cups	1.1.23_rc1	All	All
Application	Easy Software Products	Cups	1.1.22	All	All
Application	Easy Software Products	Cups	1.1.22_rc1	All	All
Application	Easy Software Products	Cups	1.1.23	All	All
Application	Easy Software Products	Cups	1.1.23_rc1	All	All
Operating System	Gentoo	Linux	All	All	All
Operating System	Gentoo	Linux	All	All	All
Application	Kde	Kdegraphics	3.2	All	All
Application	Kde	Kdegraphics	3.4.3	All	All
Application	Kde	Kdegraphics	3.2	All	All
Application	Kde	Kdegraphics	3.4.3	All	All
Application	Kde	Koffice	1.4	All	All
Application	Kde	Koffice	1.4.1	All	All
Application	Kde	Koffice	1.4.2	All	All
Application	Kde	Koffice	1.4	All	All
Application	Kde	Koffice	1.4.1	All	All
Application	Kde	Koffice	1.4.2	All	All
Application	Kde	Kpdf	3.2	All	All
Application	Kde	Kpdf	3.4.3	All	All
Application	Kde	Kpdf	3.2	All	All
Application	Kde	Kpdf	3.4.3	All	All
Application	Kde	Kword	1.4.2	All	All
Application	Kde	Kword	1.4.2	All	All
Application	Libextractor	Libextractor	All	All	All
Application	Libextractor	Libextractor	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	x86-64
Operating System	Mandrakesoft	Mandrake Linux	10.2	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.2	All	x86-64
Operating System	Mandrakesoft	Mandrake Linux	2006	All	All
Operating System	Mandrakesoft	Mandrake Linux	2006	All	x86-64
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	All

Operating System	Mandrakesoft	Mandrake Linux	10.1	All	x86-64
Operating System	Mandrakesoft	Mandrake Linux	10.2	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.2	All	x86-64
Operating System	Mandrakesoft	Mandrake Linux	2006	All	All
Operating System	Mandrakesoft	Mandrake Linux	2006	All	x86-64
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	2.1	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	2.1	All	x86_64
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	x86_64
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	2.1	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	2.1	All	x86_64
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	x86_64
Application	Poppler	Poppler	0.4.2	All	All
Application	Poppler	Poppler	0.4.2	All	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64
Operating System	Redhat	Enterprise Linux	2.1	All	workstation
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server
Operating System	Redhat	Enterprise Linux	4.0	All	workstation
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64
Operating System	Redhat	Enterprise Linux	2.1	All	workstation
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server

Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server
Operating System	Redhat	Enterprise Linux	4.0	All	workstation
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All
Operating System	Redhat	Fedora Core	core_4.0	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All
Operating System	Redhat	Fedora Core	core_4.0	All	All
Operating System	Redhat	Linux	7.3	All	i386
Operating System	Redhat	Linux	9.0	All	i386
Operating System	Redhat	Linux	7.3	All	i386
Operating System	Redhat	Linux	9.0	All	i386
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium
Operating System	Sco	Openserver	5.0.7	All	All
Operating System	Sco	Openserver	6.0	All	All
Operating System	Sco	Openserver	5.0.7	All	All
Operating System	Sco	Openserver	6.0	All	All
Application	Sgi	Propack	3.0	sp6	All
Application	Sgi	Propack	3.0	sp6	All
Operating System	Slackware	Slackware Linux	10.0	All	All
Operating System	Slackware	Slackware Linux	10.1	All	All
Operating System	Slackware	Slackware Linux	10.2	All	All
Operating System	Slackware	Slackware Linux	9.0	All	All
Operating System	Slackware	Slackware Linux	9.1	All	All
Operating System	Slackware	Slackware Linux	10.0	All	All

Operating System	Slackware	Slackware Linux	10.1	All	All
Operating System	Slackware	Slackware Linux	10.2	All	All
Operating System	Slackware	Slackware Linux	9.0	All	All
Operating System	Slackware	Slackware Linux	9.1	All	All
Operating System	Suse	Suse Linux	1.0	All	All
Operating System	Suse	Suse Linux	10.0	All	oss
Operating System	Suse	Suse Linux	10.0	All	professional
Operating System	Suse	Suse Linux	9.0	All	enterprise_server
Operating System	Suse	Suse Linux	9.0	All	personal
Operating System	Suse	Suse Linux	9.0	All	professional
Operating System	Suse	Suse Linux	9.0	All	s_390
Operating System	Suse	Suse Linux	9.0	All	x86_64
Operating System	Suse	Suse Linux	9.1	All	personal
Operating System	Suse	Suse Linux	9.1	All	professional
Operating System	Suse	Suse Linux	9.1	All	x86_64
Operating System	Suse	Suse Linux	9.2	All	personal
Operating System	Suse	Suse Linux	9.2	All	professional
Operating System	Suse	Suse Linux	9.2	All	x86_64
Operating System	Suse	Suse Linux	9.3	All	personal
Operating System	Suse	Suse Linux	9.3	All	professional
Operating System	Suse	Suse Linux	9.3	All	x86_64
Operating System	Suse	Suse Linux	1.0	All	All
Operating System	Suse	Suse Linux	10.0	All	oss
Operating System	Suse	Suse Linux	10.0	All	professional
Operating System	Suse	Suse Linux	9.0	All	enterprise_server
Operating System	Suse	Suse Linux	9.0	All	personal
Operating System	Suse	Suse Linux	9.0	All	professional
Operating System	Suse	Suse Linux	9.0	All	s_390
Operating System	Suse	Suse Linux	9.0	All	x86_64
Operating System	Suse	Suse Linux	9.1	All	personal
Operating System	Suse	Suse Linux	9.1	All	professional
Operating System	Suse	Suse Linux	9.1	All	x86_64
Operating System	Suse	Suse Linux	9.2	All	personal
Operating System	Suse	Suse Linux	9.2	All	professional
Operating System	Suse	Suse Linux	9.2	All	x86_64
Operating System	Suse	Suse Linux	9.2	All	personal

Operating System	Suse	Suse Linux	9.3	All	personal
Operating System	Suse	Suse Linux	9.3	All	professional
Operating System	Suse	Suse Linux	9.3	All	x86_64
Application	Tetex	Tetex	1.0.7	All	All
Application	Tetex	Tetex	2.0	All	All
Application	Tetex	Tetex	2.0.1	All	All
Application	Tetex	Tetex	2.0.2	All	All
Application	Tetex	Tetex	3.0	All	All
Application	Tetex	Tetex	1.0.7	All	All
Application	Tetex	Tetex	2.0	All	All
Application	Tetex	Tetex	2.0.1	All	All
Application	Tetex	Tetex	2.0.2	All	All
Application	Tetex	Tetex	3.0	All	All
Operating System	Trustix	Secure Linux	2.0	All	All
Operating System	Trustix	Secure Linux	2.2	All	All
Operating System	Trustix	Secure Linux	3.0	All	All
Operating System	Trustix	Secure Linux	2.0	All	All
Operating System	Trustix	Secure Linux	2.2	All	All
Operating System	Trustix	Secure Linux	3.0	All	All
Operating System	Turbolinux	Turbolinux	10	All	All
Operating System	Turbolinux	Turbolinux	fuji	All	All
Operating System	Turbolinux	Turbolinux	10	All	All
Operating System	Turbolinux	Turbolinux	fuji	All	All
Operating System	Turbolinux	Turbolinux Appliance Server	1.0_hosting_edition	All	All
Operating System	Turbolinux	Turbolinux Appliance Server	1.0_workgroup_edition	All	All
Operating System	Turbolinux	Turbolinux Appliance Server	1.0_hosting_edition	All	All
Operating System	Turbolinux	Turbolinux Appliance Server	1.0_workgroup_edition	All	All
Operating System	Turbolinux	Turbolinux Desktop	10.0	All	All
Operating System	Turbolinux	Turbolinux Desktop	10.0	All	All
Operating System	Turbolinux	Turbolinux Home	All	All	All
Operating System	Turbolinux	Turbolinux Home	All	All	All
Operating System	Turbolinux	Turbolinux Multimedia	All	All	All
Operating System	Turbolinux	Turbolinux Multimedia	All	All	All
Operating System	Turbolinux	Turbolinux Personal	All	All	All
Operating System	Turbolinux	Turbolinux Personal	All	All	All
Operating System	Turbolinux	Turbolinux Server	10.0	All	All

Operating System	Turbolinux	Turbolinux Server	10.0_x86	All	All
Operating System	Turbolinux	Turbolinux Server	8.0	All	All
Operating System	Turbolinux	Turbolinux Server	10.0	All	All
Operating System	Turbolinux	Turbolinux Server	10.0_x86	All	All
Operating System	Turbolinux	Turbolinux Server	8.0	All	All
Operating System	Turbolinux	Turbolinux Workstation	8.0	All	All
Operating System	Turbolinux	Turbolinux Workstation	8.0	All	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc
Operating System	Ubuntu	Ubuntu Linux	5.04	All	amd64
Operating System	Ubuntu	Ubuntu Linux	5.04	All	i386
Operating System	Ubuntu	Ubuntu Linux	5.04	All	powerpc
Operating System	Ubuntu	Ubuntu Linux	5.10	All	amd64
Operating System	Ubuntu	Ubuntu Linux	5.10	All	i386
Operating System	Ubuntu	Ubuntu Linux	5.10	All	powerpc
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc
Operating System	Ubuntu	Ubuntu Linux	5.04	All	amd64
Operating System	Ubuntu	Ubuntu Linux	5.04	All	i386
Operating System	Ubuntu	Ubuntu Linux	5.04	All	powerpc
Operating System	Ubuntu	Ubuntu Linux	5.10	All	amd64
Operating System	Ubuntu	Ubuntu Linux	5.10	All	i386
Operating System	Ubuntu	Ubuntu Linux	5.10	All	powerpc
Application	Xpdf	Xpdf	3.0	All	All
Application	Xpdf	Xpdf	3.0	All	All

References

Reference	Sour
Gentoo Linux Documentation -- Xpdf, Poppler, GPdf, libextractor, pdftohtml: Heap overflows	GEN
USN-236-1: xpdf vulnerabilities | Ubuntu security notices	UBU
Secunia - Advisories - Debian update for pdfkit.framework	SEC
[SECURITY] Fedora Core 3 Update: cups-1.1.22-0.rc1.8.9	CON
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	SEC
Advisories - Mandriva Linux OS	MAN
[SECURITY] Fedora Core 4 Update: poppler-0.4.4-1.1	FED

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	FEDO
Secunia - Advisories - Gentoo updates for xpdf/poppler/gpdf/libextractor/pdftohtml	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
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: xpdf,kpdf,gpdf,kword (SUSE-SA:2006:001)	SUSE
Debian -- Security Information -- DSA-962-1 pdftohtml	DEBI
Advisories - Mandriva Linux	MANI
rhn.redhat.com | Red Hat Support	REDH
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	GENT
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
IBM X-Force Exchange	XF
Secunia - Advisories - Fedora update for poppler	SECU

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	FEDO
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	SUNA
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	FEDO
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
Repository / Oval Repository	OVAL

scary.beasts.org/security/CESA-2005-003.txt	MISC
Secunia - Advisories - Poppler Xpdf Multiple Integer Overflow Vulnerabilities	SECU
Secunia - Advisories - Debian update for gpdf	SECU
2006-0002	TRUS
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 registred 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