



CVE-2005-3191

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2005-3191
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-07 01:03:00 UTC
Updated	2018-10-19 15:34:00 UTC
Description	Multiple heap-based buffer overflows in the (1) DCTStream::readProgressiveSOF and (2) DCTStream::readBaselineSOF fu

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xpdf	Xpdf	0.90	All	All	All
Application	Xpdf	Xpdf	0.91	All	All	All
Application	Xpdf	Xpdf	0.92	All	All	All
Application	Xpdf	Xpdf	0.93	All	All	All
Application	Xpdf	Xpdf	1.0	All	All	All
Application	Xpdf	Xpdf	1.0a	All	All	All
Application	Xpdf	Xpdf	1.1	All	All	All
Application	Xpdf	Xpdf	2.0	All	All	All
Application	Xpdf	Xpdf	2.1	All	All	All
Application	Xpdf	Xpdf	2.2	All	All	All
Application	Xpdf	Xpdf	2.3	All	All	All
Application	Xpdf	Xpdf	3.0	All	All	All
Application	Xpdf	Xpdf	3.0.1	All	All	All
Application	Xpdf	Xpdf	3.0_pl2	All	All	All
Application	Xpdf	Xpdf	3.0_pl3	All	All	All
Application	Xpdf	Xpdf	0.90	All	All	All
Application	Xpdf	Xpdf	0.91	All	All	All

Application	Xpdf	Xpdf	0.92	All	All	All
Application	Xpdf	Xpdf	0.93	All	All	All
Application	Xpdf	Xpdf	1.0	All	All	All
Application	Xpdf	Xpdf	1.0a	All	All	All
Application	Xpdf	Xpdf	1.1	All	All	All
Application	Xpdf	Xpdf	2.0	All	All	All
Application	Xpdf	Xpdf	2.1	All	All	All
Application	Xpdf	Xpdf	2.2	All	All	All
Application	Xpdf	Xpdf	2.3	All	All	All
Application	Xpdf	Xpdf	3.0	All	All	All
Application	Xpdf	Xpdf	3.0.1	All	All	All
Application	Xpdf	Xpdf	3.0_pl2	All	All	All
Application	Xpdf	Xpdf	3.0_pl3	All	All	All

References

Reference

[SECURITY] Fedora Core 3 Update: tetex-2.0.2-21.5

Accenture | Let there be change

Support

Secunia - Advisories - Debian update for pdftk.framework

Secunia - Advisories - Xpdf Multiple Buffer Overflow Vulnerabilities

SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia

Advisories - Mandriva Linux OS

Secunia - Advisories - Red Hat update for kdegraphics

[SECURITY] Fedora Core 3 Update: cups-1.1.22-0.rc1.8.8

XPDF DCTStream Progressive Remote Heap Buffer Overflow Vulnerability

Secunia - Advisories - Debian update for tetex-bin

Accenture | Let there be change

Webmail - OVH

Multiple Vendor xpdf DCTStream Baseline Heap Overflow Vulnerability - CXSecurity.com

Debian -- Security Information -- DSA-936-1 libextractor

Secunia - Advisories - GNOME gpdf Xpdf Buffer Overflow Vulnerabilities

Secunia - Advisories - Mandriva update for cups

SecurityFocus

SUSE update for multiple packages - Advisories - Secunia

Debian -- Page not found
Secunia - Advisories - xpdf Multiple Integer Overflow Vulnerabilities
Webmail - OVH
IBM X-Force Exchange
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: xpdf,kpdf,gpdf,kword (SUSE-SA:2006:001)
Multiple Vendor xpdf DCTStream Progressive Heap Overflow - CXSecurity.com
Debian -- Security Information -- DSA-962-1 pdftohtml
Advisories - Mandriva Linux
rhn.redhat.com Red Hat Support
IBM X-Force Exchange
Secunia - Advisories - KOffice KWord PDF Filter Xpdf Buffer Overflow Vulnerabilities
Secunia - Advisories - Fedora update for xpdf
Secunia - Advisories - Slackware update for xpdf
Webmail - OVH
Advisories - Mandriva Linux OS
20060201-01-U
SecurityFocus
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates
20051201-01-U
Secunia - Advisories - CUPS xpdf Multiple Buffer Overflow Vulnerabilities
#342289 - xpdf security problems partially affect pdftohtml as well - Debian Bug report logs
[SECURITY] Fedora Core 4 Update: cups-1.1.23-15.2
20060101-01-U
Gentoo Linux Documentation -- Xpdf, GPdf, CUPS, Poppler: Multiple vulnerabilities
Secunia - Advisories - Red Hat update for xpdf
TLSA-2005-0072
Secunia - Advisories - Gentoo updates for xpdf / gpdf / cups / poppler
Advisories - Mandriva Linux OS
Repository / Oval Repository
Advisories - Mandriva Linux OS
Secunia - Advisories - Debian update for libextractor
www.kde.org/info/security/advisory-20051207-1.txt
Sun Solaris Gnome PDF Viewer Multiple Vulnerabilities - Advisories - Secunia
[SECURITY] Fedora Core 4 Update: tetex-3.0-7.FC4
Debian -- Page not found
Debian -- Page not found

Gentoo Linux Documentation -- KPdf, KWord: Multiple overflows in included Xpdf code
Secunia - Advisories - Debian update for kpdf
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates
Secunia - Advisories - Red Hat update for cups
Security Announcement
Security Announcement
The Slackware Linux Project: Slackware Security Advisories
Debian -- Page not found
rhn.redhat.com Red Hat Support
Secunia - Advisories - Debian update for koffice
Secunia - Advisories - UnixWare update for CUPS
Secunia - Advisories - Gentoo update for kdegraphics / kpdf / koffice / kword
102972
www.kde.org/info/security/advisory-20051207-2.txt
Debian -- Page not found
Secunia - Advisories - Fedora update for tetex
SecurityTracker.com Archives - KDE KOffice kpdf Buffer Overflows in Processing DCT and JPX Streams May Let Remote Users Execute Arbitrary Code
Advisories - Mandriva Linux OS
Advisories - Mandriva Linux OS
SCOSA-2006.20
The Slackware Linux Project: Slackware Security Advisories
Advisories - Mandriva Linux OS
Webmail - OVH
Secunia - Advisories - libextractor Multiple Xpdf Vulnerabilities
Secunia - Advisories - SCO OpenServer update for CUPS
Secunia - Advisories - SUSE updates for xpdf / kpdf / gpdf / kword
Secunia - Advisories - Debian update for pdftohtml
USN-227-1: xpdf vulnerabilities Ubuntu security notices Ubuntu
Secunia - Advisories - pdftohtml Xpdf Buffer Overflow Vulnerabilities
Debian -- Security Information -- DSA-961-1 pdftkit.framework
Secunia - Advisories - SUSE update for multiple packages
Secunia - Advisories - Red Hat update for tetex
Secunia - Advisories - teTeX Xpdf Buffer Overflow Vulnerabilities
Secunia - Advisories - Debian update for cupsys
Secunia - Advisories - Slackware update for kdegraphics

Secunia - Advisories - Mandriva update for xpdf
Secunia - Advisories - Ubuntu updates for xpdf / cupsys / tetex-bin / kdegraphics / koffice
Secunia - Advisories - GNUStep PDFKit Framework Xpdf Multiple Vulnerabilities
XPDF DCTStream Baseline Remote Heap Buffer Overflow Vulnerability
Secunia - Advisories - Debian update for xpdf
Secunia - Advisories - KDE kpdf Xpdf Buffer Overflow Vulnerabilities
Webmail - OVH
rhn.redhat.com Red Hat Support
Secunia - Advisories - Poppler Xpdf Buffer Overflow Vulnerabilities
rhn.redhat.com Red Hat Support
SCOSA-2006.15
SecurityFocus
SCOSA-2006.21
Secunia - Advisories - Trustix update for cups / curl
Secunia - Advisories - Mandriva update for tetex
Webmail - OVH
Debian -- Security Information -- DSA-950-1 cupsys
SecurityTracker.com Archives - Xpdf Buffer Overflows in Processing DCT and JPX Streams May Let Remote Users Execute Arbitrary Code
rPath update for cups, poppler, and tetex - Advisories - Secunia
Red Hat update for gpdf - Secunia Advisories - Vulnerability Intelligence - Secunia.com
issues.rpath.com/browse/RPL-1609
Secunia - Advisories - Debian update for gpdf
Webmail - OVH
Secunia - Advisories - Fedora update for cups
Secunia - Advisories - Fedora update for tetex
SCO OpenServer update for xpdf - Advisories - Secunia
CVE Program record
NVD vulnerability detail

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](#)