CVE-2009-3608

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2009-3608
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-21 17:30:00 UTC
Updated	2023-02-13 02:20:00 UTC
Description	Integer overflow in the ObjectStream::ObjectStream function in XRef.cc in Xpdf 3.x before 3.02pl4 and Poppler before 0.12.

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Foolabs	Xpdf	3.02pl1	All	All	All
Application	Foolabs	Xpdf	3.02pl2	All	All	All
Application	Foolabs	Xpdf	3.02pl3	All	All	All
Application	Foolabs	Xpdf	3.02pl1	All	All	All
Application	Foolabs	Xpdf	3.02pl2	All	All	All
Application	Foolabs	Xpdf	3.02pl3	All	All	All
Application	Glyphandcog	Xpdfreader	3.00	All	All	All
Application	Glyphandcog	Xpdfreader	3.01	All	All	All
Application	Glyphandcog	Xpdfreader	3.02	All	All	All
Application	Glyphandcog	Xpdfreader	3.00	All	All	All
Application	Glyphandcog	Xpdfreader	3.01	All	All	All
Application	Glyphandcog	Xpdfreader	3.02	All	All	All
Application	Glyph And Cog	Pdftops	All	All	All	All
Application	Glyph And Cog	Pdftops	All	All	All	All
Application	Gnome	Gpdf	All	All	All	All
Application	Gnome	Gpdf	All	All	All	All
Application	Kde	Kpdf	All	All	All	All

Application	Kde	Kpdf	All	All	All	All
Application	Poppler	Poppler	0.1	All	All	All
Application	Poppler	Poppler	0.1.1	All	All	All
Application	Poppler	Poppler	0.1.2	All	All	All
Application	Poppler	Poppler	0.10.0	All	All	All
Application	Poppler	Poppler	0.10.1	All	All	All
Application	Poppler	Poppler	0.10.2	All	All	All
Application	Poppler	Poppler	0.10.3	All	All	All
Application	Poppler	Poppler	0.10.4	All	All	All
Application	Poppler	Poppler	0.10.5	All	All	All
Application	Poppler	Poppler	0.10.6	All	All	All
Application	Poppler	Poppler	0.10.7	All	All	All
Application	Poppler	Poppler	0.11.0	All	All	All
Application	Poppler	Poppler	0.11.1	All	All	All
Application	Poppler	Poppler	0.11.2	All	All	All
Application	Poppler	Poppler	0.11.3	All	All	All
Application	Poppler	Poppler	0.2.0	All	All	All
Application	Poppler	Poppler	0.3.0	All	All	All
Application	Poppler	Poppler	0.3.1	All	All	All
Application	Poppler	Poppler	0.3.2	All	All	All
Application	Poppler	Poppler	0.3.3	All	All	All
Application	Poppler	Poppler	0.4.0	All	All	All
Application	Poppler	Poppler	0.4.1	All	All	All
Application	Poppler	Poppler	0.4.2	All	All	All
Application	Poppler	Poppler	0.4.3	All	All	All
Application	Poppler	Poppler	0.4.4	All	All	All
Application	Poppler	Poppler	0.5.0	All	All	All
Application	Poppler	Poppler	0.5.1	All	All	All
Application	Poppler	Poppler	0.5.2	All	All	All
Application	Poppler	Poppler	0.5.3	All	All	All
Application	Poppler	Poppler	0.5.4	All	All	All
Application	Poppler	Poppler	0.5.9	All	All	All
Application	Poppler	Poppler	0.6.0	All	All	All
Application	Poppler	Poppler	0.6.1	All	All	All
Application	Poppler	Poppler	0.6.2	All	All	All

Application	Poppler	Poppler	0.6.3	All	All	All
Application	Poppler	Poppler	0.6.4	All	All	All
Application	Poppler	Poppler	0.7.0	All	All	All
Application	Poppler	Poppler	0.7.1	All	All	All
Application	Poppler	Poppler	0.7.2	All	All	All
Application	Poppler	Poppler	0.7.3	All	All	All
Application	Poppler	Poppler	0.8.0	All	All	All
Application	Poppler	Poppler	0.8.1	All	All	All
Application	Poppler	Poppler	0.8.2	All	All	All
Application	Poppler	Poppler	0.8.3	All	All	All
Application	Poppler	Poppler	0.8.4	All	All	All
Application	Poppler	Poppler	0.8.6	All	All	All
Application	Poppler	Poppler	0.8.7	All	All	All
Application	Poppler	Poppler	0.9.0	All	All	All
Application	Poppler	Poppler	0.9.1	All	All	All
Application	Poppler	Poppler	0.9.2	All	All	All
Application	Poppler	Poppler	0.9.3	All	All	All
Application	Poppler	Poppler	All	All	All	All
Application	Poppler	Poppler	0.1	All	All	All
Application	Poppler	Poppler	0.1.1	All	All	All
Application	Poppler	Poppler	0.1.2	All	All	All
Application	Poppler	Poppler	0.10.0	All	All	All
Application	Poppler	Poppler	0.10.1	All	All	All
Application	Poppler	Poppler	0.10.2	All	All	All
Application	Poppler	Poppler	0.10.3	All	All	All
Application	Poppler	Poppler	0.10.4	All	All	All
Application	Poppler	Poppler	0.10.5	All	All	All
Application	Poppler	Poppler	0.10.6	All	All	All
Application	Poppler	Poppler	0.10.7	All	All	All
Application	Poppler	Poppler	0.11.0	All	All	All
Application	Poppler	Poppler	0.11.1	All	All	All
Application	Poppler	Poppler	0.11.2	All	All	All
Application	Poppler	Poppler	0.11.3	All	All	All
Application	Poppler	Poppler	0.2.0	All	All	All
Application	Poppler	Poppler	0.3.0	All	All	All

Application	Poppler	Poppler	0.3.1	All	All	All
Application	Poppler	Poppler	0.3.2	All	All	All
Application	Poppler	Poppler	0.3.3	All	All	All
Application	Poppler	Poppler	0.4.0	All	All	All
Application	Poppler	Poppler	0.4.1	All	All	All
Application	Poppler	Poppler	0.4.2	All	All	All
Application	Poppler	Poppler	0.4.3	All	All	All
Application	Poppler	Poppler	0.4.4	All	All	All
Application	Poppler	Poppler	0.5.0	All	All	All
Application	Poppler	Poppler	0.5.1	All	All	All
Application	Poppler	Poppler	0.5.2	All	All	All
Application	Poppler	Poppler	0.5.3	All	All	All
Application	Poppler	Poppler	0.5.4	All	All	All
Application	Poppler	Poppler	0.5.9	All	All	All
Application	Poppler	Poppler	0.6.0	All	All	All
Application	Poppler	Poppler	0.6.1	All	All	All
Application	Poppler	Poppler	0.6.2	All	All	All
Application	Poppler	Poppler	0.6.3	All	All	All
Application	Poppler	Poppler	0.6.4	All	All	All
Application	Poppler	Poppler	0.7.0	All	All	All
Application	Poppler	Poppler	0.7.1	All	All	All
Application	Poppler	Poppler	0.7.2	All	All	All
Application	Poppler	Poppler	0.7.3	All	All	All
Application	Poppler	Poppler	0.8.0	All	All	All
Application	Poppler	Poppler	0.8.1	All	All	All
Application	Poppler	Poppler	0.8.2	All	All	All
Application	Poppler	Poppler	0.8.3	All	All	All
Application	Poppler	Poppler	0.8.4	All	All	All
Application	Poppler	Poppler	0.8.6	All	All	All
Application	Poppler	Poppler	0.8.7	All	All	All
Application	Poppler	Poppler	0.9.0	All	All	All
Application	Poppler	Poppler	0.9.1	All	All	All
Application	Poppler	Poppler	0.9.2	All	All	All
Application	Poppler	Poppler	0.9.3	All	All	All
Application	Tetex	Tetex	All	All	All	All
Application	Tetex	Tetex	All	All	All	All

References

Reference	Source
[SECURITY] Fedora 11 Update: pdfedit-0.4.3-4.fc11	FEDORA
Red Hat Customer Portal	MISC
Debian update for kdegraphics - Advisories - Community	SECUNIA
SecurityTracker.com Archives - Xpdf Integer Overflows Let Remote Users Execute Arbitrary Code	SECTRACK
rhn.redhat.com | Red Hat Support	REDHAT
KDE KPDF Multiple Vulnerabilities - Secunia.com	SECUNIA
Red Hat Customer Portal	MISC
Red Hat update for xpdf - Secunia.com	SECUNIA
Fedora update for poppler - Secunia.com	SECUNIA
oCERT.org - oCERT Advisories	MISC
rhn.redhat.com | Red Hat Support	REDHAT
Ubuntu update for poppler - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Poppler Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
CUPS "pdftops" Two Integer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
[SECURITY] Fedora 12 Update: pdfedit-0.4.3-4.fc12	FEDORA
Red Hat Customer Portal	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Debian -- Security Information -- DSA-1941-1 poppler	DEBIAN
Repository / Oval Repository	OVAL
526637 – (CVE-2009-3608) CVE-2009-3608 xpdf/poppler: integer overflow in ObjectStream::ObjectStream (oCERT-2009-016)	CONFIRM
Red Hat Customer Portal	MISC
Support / Security / Advisories / / MDVSA-2011:175 | Mandriva	MANDRIVA
USN-850-1: poppler vulnerabilities | Ubuntu	UBUNTU
[SECURITY] Fedora 13 Update: pdfedit-0.4.3-4.fc13	FEDORA
oss-security - Re: Need more information on recent poppler issues	MLIST
rhn.redhat.com | Red Hat Support	REDHAT
Red Hat update for kdegraphics - Secunia.com	SECUNIA
[SECURITY] Fedora 10 Update: poppler-0.8.7-7.fc10	FEDORA
rhn.redhat.com | Red Hat Support	REDHAT
Debian -- Security Information -- DSA-2050-1 kdegraphics	DEBIAN
Webmail | OVH- OVH	VUPEN
USN-850-3: poppler vulnerabilities | Ubuntu	UBUNTU
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	SUSE

[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	SUSE
IBM X-Force Exchange	XF
rhn.redhat.com | Red Hat Support	REDHAT
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Red Hat update for cups - Secunia.com	SECUNIA
Red Hat update for poppler - Secunia.com	SECUNIA
Debian update for xpdf - Advisories - Community	SECUNIA
Poppler	CONFIRM
oss-security - Re: Need more information on recent poppler issues	MLIST
Red Hat update for gpdf - Secunia.com	SECUNIA
1021706	SUNALERT
Webmail | OVH- OVH	VUPEN
Xpdf Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
274030	SUNALERT
Debian -- Security Information -- DSA-2028-1 xpdf	DEBIAN
oss-security - Need more information on recent poppler issues	MLIST
rhn.redhat.com | Red Hat Support	REDHAT
Xpdf Multiple Integer Overflow Vulnerabilities	BID
Webmail | OVH- OVH	VUPEN
Red Hat Customer Portal	MISC
access.redhat.com | CVE-2009-3608	MISC
Red Hat update for kdegraphics - Secunia.com	SECUNIA
Support / Security / Advisories / / MDVSA-2009:287 | Mandriva	MANDRIVA
Red Hat Customer Portal	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Support / Security / Advisories / / MDVSA-2009:334 | Mandriva	MANDRIVA
ftp.foolabs.com/pub/xpdf/xpdf-3.02pl4.patch	CONFIRM
[SECURITY] Fedora 11 Update: poppler-0.10.7-3.fc11	FEDORA
Webmail - OVH	VUPEN
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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