CVE-2009-3609

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2009-3609
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 ImageStream::ImageStream function in Stream.cc in Xpdf before 3.02pl4 and Poppler before 0.12.1,

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

References

Reference	Source	Link
Red Hat Customer Portal	MISC	access.r
[SECURITY] Fedora 11 Update: pdfedit-0.4.3-4.fc11	FEDORA	lists.fedc
Red Hat Customer Portal	MISC	access.r
Debian update for kdegraphics - Advisories - Community	SECUNIA	secunia.
SecurityTracker.com Archives - Xpdf Integer Overflows Let Remote Users Execute Arbitrary Code	SECTRACK	securityt
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redh
KDE KPDF Multiple Vulnerabilities - Secunia.com	SECUNIA	secunia.
Red Hat Customer Portal	MISC	access.r
Red Hat Customer Portal	MISC	access.r
Red Hat update for xpdf - Secunia.com	SECUNIA	secunia.
Fedora update for poppler - Secunia.com	SECUNIA	secunia.
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redh
Ubuntu update for poppler - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.
Poppler Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.
access.redhat.com | CVE-2009-3609	MISC	access.r
CUPS "pdftops" Two Integer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.
[SECURITY] Fedora 12 Update: pdfedit-0.4.3-4.fc12	FEDORA	lists.fedc
Red Hat Customer Portal	MISC	access.r
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vup
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redh
Red Hat Customer Portal	MISC	access.r
Support / Security / Advisories / / MDVSA-2011:175 | Mandriva	MANDRIVA	www.ma
USN-850-1: poppler vulnerabilities | Ubuntu	UBUNTU	www.ubu
Repository / Oval Repository	OVAL	oval.cise
[SECURITY] Fedora 13 Update: pdfedit-0.4.3-4.fc13	FEDORA	lists.fedc
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redh
Red Hat update for kdegraphics - Secunia.com	SECUNIA	secunia.
[SECURITY] Fedora 10 Update: poppler-0.8.7-7.fc10	FEDORA	www.rec
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redh
Debian -- Security Information -- DSA-2050-1 kdegraphics	DEBIAN	www.deb
526893 – (CVE-2009-3609) CVE-2009-3609 xpdf/poppler: ImageStream::ImageStream integer overflow	CONFIRM	bugzilla.
Webmail | OVH- OVH	VUPEN	www.vup
IBM X-Force Exchange	XF	exchang
USN-850-3: poppler vulnerabilities | Ubuntu	UBUNTU	www.ubu
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	SUSE	lists.ope

[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	SUSE	lists.ope
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redh
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vup
Red Hat update for cups - Secunia.com	SECUNIA	secunia.
Red Hat update for poppler - Secunia.com	SECUNIA	secunia.
Debian update for xpdf - Advisories - Community	SECUNIA	secunia.
Poppler	CONFIRM	poppler.f
Support	REDHAT	www.rec
Repository / Oval Repository	OVAL	oval.cise
Red Hat update for gpdf - Secunia.com	SECUNIA	secunia.
1021706	SUNALERT	sunsolve
Webmail | OVH- OVH	VUPEN	www.vup
274030	SUNALERT	sunsolve
Debian -- Security Information -- DSA-2028-1 xpdf	DEBIAN	www.deb
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redh
Xpdf Multiple Integer Overflow Vulnerabilities	BID	www.sec
Webmail | OVH- OVH	VUPEN	www.vup
Red Hat Customer Portal	MISC	access.r
Red Hat update for kdegraphics - Secunia.com	SECUNIA	secunia.
Support / Security / Advisories / / MDVSA-2009:287 | Mandriva	MANDRIVA	www.ma
Red Hat Customer Portal	MISC	access.r
Red Hat Customer Portal	MISC	access.r
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.r
Support / Security / Advisories / / MDVSA-2009:334 | Mandriva	MANDRIVA	www.ma
ftp.foolabs.com/pub/xpdf/xpdf-3.02pl4.patch	CONFIRM	ftp.foolab
[SECURITY] Fedora 11 Update: poppler-0.10.7-3.fc11	FEDORA	www.rec
Red Hat Customer Portal	MISC	access.r
Red Hat update for xpdf - Secunia.com	SECUNIA	secunia.
Webmail - OVH	VUPEN	www.vup
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

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