CVE-2009-3606

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2009-3606
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 PSOutputDev::doImageL1Sep function in Xpdf before 3.02pl4, and Poppler 0.x, as used in kdegraph

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	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	0.12.0	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	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	0.12.0	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.redh
[SECURITY] Fedora 11 Update: pdfedit-0.4.3-4.fc11	FEDORA	lists.fedorap

Debian update for kdegraphics - Advisories - Community	SECUNIA	secunia.com
SecurityTracker.com Archives - Xpdf Integer Overflows Let Remote Users Execute Arbitrary Code	SECTRACK	securitytrack
Red Hat Customer Portal	MISC	access.redh
KDE KPDF Multiple Vulnerabilities - Secunia.com	SECUNIA	secunia.com
526877 – (CVE-2009-3606) CVE-2009-3606 xpdf/poppler: PSOutputDev::doImageL1Sep integer overflow	CONFIRM	bugzilla.redh
access.redhat.com | CVE-2009-3606	MISC	access.redh
Red Hat Customer Portal	MISC	access.redh
Red Hat update for xpdf - Secunia.com	SECUNIA	secunia.com
Support / Security / Advisories / / MDVSA-2010:087 | Mandriva	MANDRIVA	www.mandri
Fedora update for poppler - Secunia.com	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecuri
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redhat.c
IBM X-Force Exchange	XF	exchange.xf
Repository / Oval Repository	OVAL	oval.cisecuri
[SECURITY] Fedora 12 Update: pdfedit-0.4.3-4.fc12	FEDORA	lists.fedorap
Red Hat Customer Portal	MISC	access.redh
poppler/poppler - The poppler pdf rendering library (mirrored from https://gitlab.freedesktop.org/poppler/poppler)	CONFIRM	cgit.freedesk
Debian -- Security Information -- DSA-1941-1 poppler	DEBIAN	www.debian
Poppler Multiple Vulnerabilities - Secunia.com	SECUNIA	secunia.com
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redhat.c
Support / Security / Advisories / / MDVSA-2011:175 | Mandriva	MANDRIVA	www.mandri
[SECURITY] Fedora 13 Update: pdfedit-0.4.3-4.fc13	FEDORA	lists.fedorap
oss-security - Re: Need more information on recent poppler issues	MLIST	www.openw
Red Hat update for kdegraphics - Secunia.com	SECUNIA	secunia.com
[SECURITY] Fedora 10 Update: poppler-0.8.7-7.fc10	FEDORA	www.redhat.
Debian -- Security Information -- DSA-2050-1 kdegraphics	DEBIAN	www.debian
Webmail | OVH- OVH	VUPEN	www.vupen.
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	SUSE	lists.opensus
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redhat.c
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.
Debian update for xpdf - Advisories - Community	SECUNIA	secunia.com
oss-security - Re: Need more information on recent poppler issues	MLIST	www.openw
Red Hat Customer Portal	MISC	access.redh
1021706	SUNALERT	sunsolve.su
Webmail | OVH- OVH	VUPEN	www.vupen.
Xpdf Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com

Xpdf Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
274030	SUNALERT	sunsolve.su
Debian -- Security Information -- DSA-2028-1 xpdf	DEBIAN	www.debian
oss-security - Need more information on recent poppler issues	MLIST	www.openw
Xpdf Multiple Integer Overflow Vulnerabilities	BID	www.securit
Webmail | OVH- OVH	VUPEN	www.vupen.
Support / Security / Advisories / / MDVSA-2009:287 | Mandriva	MANDRIVA	www.mandri
ftp.foolabs.com/pub/xpdf/xpdf-3.02pl4.patch	CONFIRM	ftp.foolabs.c
[SECURITY] Fedora 11 Update: poppler-0.10.7-3.fc11	FEDORA	www.redhat.
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.
Red Hat update for xpdf - Secunia.com	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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