



CVE-2009-3604

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2009-3604
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 01:17:00 UTC
Description	The Splash::drawImage function in Splash.cc in Xpdf 2.x and 3.x before 3.02pl4, and Poppler 0.x, as used in GPdf and kde

Risk And Classification

Problem Types: CWE-399

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	2.00	All	All	All
Application	Glyphandcog	Xpdfreader	2.01	All	All	All
Application	Glyphandcog	Xpdfreader	2.02	All	All	All
Application	Glyphandcog	Xpdfreader	2.03	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	2.00	All	All	All
Application	Glyphandcog	Xpdfreader	2.01	All	All	All
Application	Glyphandcog	Xpdfreader	2.02	All	All	All
Application	Glyphandcog	Xpdfreader	2.03	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	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	0.12.0	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	0.5.90	All	All	All
Application	Poppler	Poppler	0.5.91	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	0.8.5	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	0.10.5	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	0.5.90	All	All	All
Application	Poppler	Poppler	0.5.91	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	0.8.5	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
Red Hat Customer Portal	M
[SECURITY] Fedora 11 Update: pdfedit-0.4.3-4.fc11	FI
site.pi3.com.pl/adv/xpdf.txt	M
Debian update for kdegraphics - Advisories - Community	SI
SecurityTracker.com Archives - Xpdf Integer Overflows Let Remote Users Execute Arbitrary Code	SI
KDE KPDF Multiple Vulnerabilities - Secunia.com	SI
access.redhat.com CVE-2009-3604	M
Red Hat Customer Portal	M
Red Hat update for xpdf - Secunia.com	SI
Support / Security / Advisories // MDVSA-2010:087 Mandriva	M
Fedora update for poppler - Secunia.com	SI
rh.n.redhat.com Red Hat Support	R
Ubuntu update for poppler - Secunia Advisories - Vulnerability Information - Secunia.com	SI
[SECURITY] Fedora 12 Update: pdfedit-0.4.3-4.fc12	FI
Red Hat Customer Portal	M
Poppler Multiple Vulnerabilities - Secunia.com	SI
rh.n.redhat.com Red Hat Support	R
Red Hat Customer Portal	M
Support / Security / Advisories // MDVSA-2011:175 Mandriva	M
USN-850-1: poppler vulnerabilities Ubuntu	U
526911 – (CVE-2009-3604) CVE-2009-3604 xpdf/poppler: Splash::drawImage integer overflow and missing allocation return value check	C
poppler/poppler: The poppler pdf rendering library (mirrored from https://github.com/freedesktop.org/poppler/poppler)	C

poppler/poppler - The poppler pdf rendering library (mirrored from https://gitlab.freedesktop.org/poppler/poppler)	C
[SECURITY] Fedora 13 Update: pdfedit-0.4.3-4.fc13	FI
rhn.redhat.com Red Hat Support	R
Red Hat update for kdegraphics - Secunia.com	SI
[SECURITY] Fedora 10 Update: poppler-0.8.7-7.fc10	FI
Debian -- Security Information -- DSA-2050-1 kdegraphics	D
Webmail OVH- OVH	VI
USN-850-3: poppler vulnerabilities Ubuntu	U
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	SI
rhn.redhat.com Red Hat Support	R
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VI
Repository / Oval Repository	O
Debian update for xpdf - Advisories - Community	SI
IBM X-Force Exchange	XI
Red Hat Customer Portal	M
Red Hat update for gpdf - Secunia.com	SI
1021706	SI
Webmail OVH- OVH	VI
Xpdf Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SI
274030	SI
Debian -- Security Information -- DSA-2028-1 xpdf	D
poppler/poppler - The poppler pdf rendering library (mirrored from https://gitlab.freedesktop.org/poppler/poppler)	C
rhn.redhat.com Red Hat Support	R
Xpdf Multiple Integer Overflow Vulnerabilities	BI
Webmail OVH- OVH	VI
Red Hat Customer Portal	M
Red Hat update for kdegraphics - Secunia.com	SI
Support / Security / Advisories // MDVSA-2009:287 Mandriva	M
ftp.foolabs.com/pub/xpdf/xpdf-3.02pl4.patch	C
[SECURITY] Fedora 11 Update: poppler-0.10.7-3.fc11	FI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VI
Red Hat update for xpdf - Secunia.com	SI
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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](#)