



CVE-2009-3603

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

Summary

CVE	CVE-2009-3603
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-21 17:30:00 UTC
Updated	2023-11-07 02:04:00 UTC
Description	Integer overflow in the SplashBitmap::SplashBitmap function in Xpdf 3.x before 3.02pl4 and Poppler before 0.12.1 might all

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	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

Support / Security / Advisories // MDVSA-2010:087 Mandriva	MANDRIVA	www.mandriva.com
Fedora update for poppler - Secunia.com	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
Ubuntu update for poppler - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Poppler Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
[SECURITY] Fedora 12 Update: pdfedit-0.4.3-4.fc12	FEDORA	lists.fedoraproject.c
IBM X-Force Exchange	XF	exchange.xforce.ibm
Support / Security / Advisories // MDVSA-2011:175 Mandriva	MANDRIVA	www.mandriva.com
USN-850-1: poppler vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
[SECURITY] Fedora 13 Update: pdfedit-0.4.3-4.fc13	FEDORA	lists.fedoraproject.c
526915 – (CVE-2009-3603) CVE-2009-3603 xpdf/poppler: SplashBitmap::SplashBitmap integer overflow	CONFIRM	bugzilla.redhat.com
[SECURITY] Fedora 10 Update: poppler-0.8.7-7.fc10	FEDORA	www.redhat.com
rhn.redhat.com Red Hat Support	REDHAT	rhn.redhat.com
Debian -- Security Information -- DSA-2050-1 kdegraphics	DEBIAN	www.debian.org
Webmail OVH- OVH	VUPEN	www.vupen.com
USN-850-3: poppler vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	SUSE	lists.opensuse.org
Red Hat update for poppler - Secunia.com	SECUNIA	secunia.com
Debian update for xpdf - Advisories - Community	SECUNIA	secunia.com
Poppler	CONFIRM	poppler.freedesktop
1021706	SUNALERT	sunsolve.sun.com
Webmail OVH- OVH	VUPEN	www.vupen.com
Xpdf Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
274030	SUNALERT	sunsolve.sun.com
Debian -- Security Information -- DSA-2028-1 xpdf	DEBIAN	www.debian.org
Xpdf Multiple Integer Overflow Vulnerabilities	BID	www.securityfocus.
Webmail OVH- OVH	VUPEN	www.vupen.com
Support / Security / Advisories // MDVSA-2009:287 Mandriva	MANDRIVA	www.mandriva.com
ftp.foolabs.com/pub/xpdf/xpdf-3.02pl4.patch	CONFIRM	ftp.foolabs.com
[SECURITY] Fedora 11 Update: poppler-0.10.7-3.fc11	FEDORA	www.redhat.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Webmail - OVH	VUPEN	www.vupen.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.

© [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](#)