



CVE-2009-3607

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

Summary

CVE	CVE-2009-3607
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 create_surface_from_thumbnail_data function in glib/poppler-page.cc in Poppler 0.x allows remote a

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	0.10.6	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	0.5.20	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	Link
poppler/poppler - The poppler pdf rendering library	CONFIRM	cgit.freedesktop.org
Fedora update for poppler - Secunia.com	SECUNIA	secunia.com
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
Bug 526924 – CVE-2009-3607 poppler: create_surface_from_thumbnail_data integer overflow	CONFIRM	bugzilla.redhat.com
Debian -- Security Information -- DSA-1941-1 poppler	DEBIAN	www.debian.org
Poppler 'create_surface_from_thumbnail_data()' Integer Overflow Memory Corruption Vulnerability	BID	www.securityfocus.com
Support / Security / Advisories // MDVSA-2011:175 Mandriva	MANDRIVA	www.mandriva.com
USN-850-1: poppler vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
oss-security - Re: Need more information on recent poppler issues	MLIST	www.openwall.com

[SECURITY] Fedora 10 Update: poppler-0.8.7-7.fc10	FEDORA	www.redhat.com
USN-850-3: poppler vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
CVE-2009-3607 - Red Hat Customer Portal	MISC	access.redhat.com
oss-security - Re: Need more information on recent poppler issues	MLIST	www.openwall.com
1021706	SUNALERT	sunsolve.sun.com
274030	SUNALERT	sunsolve.sun.com
oss-security - Need more information on recent poppler issues	MLIST	www.openwall.com
[SECURITY] Fedora 11 Update: poppler-0.10.7-3.fc11	FEDORA	www.redhat.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Webmail - OVH	VUPEN	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-10-23	Tomas Hoger	Not vulnerable. This issue did not affect the version of poppler as shipped with Red Hat Enterprise Linux 5.5.

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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org/cve). This site includes MITRE data granted under the following [license](http://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report