



CVE-2013-4243

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

Summary

CVE	CVE-2013-4243
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-09-10 19:55:00 UTC
Updated	2023-02-13 04:45:00 UTC
Description	Heap-based buffer overflow in the readgifimage function in the gif2tiff tool in libtiff 4.0.3 and earlier allows remote attackers

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Libtiff	Libtiff	3.4	All	All	All
Application	Libtiff	Libtiff	3.4	beta18	All	All
Application	Libtiff	Libtiff	3.4	beta24	All	All
Application	Libtiff	Libtiff	3.4	beta28	All	All
Application	Libtiff	Libtiff	3.4	beta29	All	All
Application	Libtiff	Libtiff	3.4	beta31	All	All
Application	Libtiff	Libtiff	3.4	beta32	All	All
Application	Libtiff	Libtiff	3.4	beta34	All	All
Application	Libtiff	Libtiff	3.4	beta35	All	All
Application	Libtiff	Libtiff	3.4	beta36	All	All
Application	Libtiff	Libtiff	3.4	beta37	All	All
Application	Libtiff	Libtiff	3.5.1	All	All	All
Application	Libtiff	Libtiff	3.5.2	All	All	All

Application	Libtiff	Libtiff	3.5.3	All	All	All
Application	Libtiff	Libtiff	3.5.4	All	All	All
Application	Libtiff	Libtiff	3.5.5	All	All	All
Application	Libtiff	Libtiff	3.5.6	All	All	All
Application	Libtiff	Libtiff	3.5.6	beta	All	All
Application	Libtiff	Libtiff	3.5.7	All	All	All
Application	Libtiff	Libtiff	3.5.7	alpha	All	All
Application	Libtiff	Libtiff	3.5.7	alpha2	All	All
Application	Libtiff	Libtiff	3.5.7	alpha3	All	All
Application	Libtiff	Libtiff	3.5.7	alpha4	All	All
Application	Libtiff	Libtiff	3.5.7	beta	All	All
Application	Libtiff	Libtiff	3.6.0	All	All	All
Application	Libtiff	Libtiff	3.6.0	beta	All	All
Application	Libtiff	Libtiff	3.6.0	beta2	All	All
Application	Libtiff	Libtiff	3.6.1	All	All	All
Application	Libtiff	Libtiff	3.7.0	All	All	All
Application	Libtiff	Libtiff	3.7.0	alpha	All	All
Application	Libtiff	Libtiff	3.7.0	beta	All	All
Application	Libtiff	Libtiff	3.7.0	beta2	All	All
Application	Libtiff	Libtiff	3.7.1	All	All	All
Application	Libtiff	Libtiff	3.7.2	All	All	All
Application	Libtiff	Libtiff	3.7.3	All	All	All
Application	Libtiff	Libtiff	3.7.4	All	All	All
Application	Libtiff	Libtiff	3.8.0	All	All	All
Application	Libtiff	Libtiff	3.8.1	All	All	All
Application	Libtiff	Libtiff	3.8.2	All	All	All
Application	Libtiff	Libtiff	3.9	All	All	All
Application	Libtiff	Libtiff	3.9.0	All	All	All
Application	Libtiff	Libtiff	3.9.0	beta	All	All
Application	Libtiff	Libtiff	3.9.1	All	All	All
Application	Libtiff	Libtiff	3.9.2	All	All	All
Application	Libtiff	Libtiff	3.9.2-5.2.1	All	All	All
Application	Libtiff	Libtiff	3.9.3	All	All	All
Application	Libtiff	Libtiff	3.9.4	All	All	All
Application	Libtiff	Libtiff	3.9.5	All	All	All

Application	Libtiff	Libtiff	4.0	All	All	All
Application	Libtiff	Libtiff	4.0	alpha	All	All
Application	Libtiff	Libtiff	4.0	beta1	All	All
Application	Libtiff	Libtiff	4.0	beta2	All	All
Application	Libtiff	Libtiff	4.0	beta3	All	All
Application	Libtiff	Libtiff	4.0	beta4	All	All
Application	Libtiff	Libtiff	4.0	beta5	All	All
Application	Libtiff	Libtiff	4.0	beta6	All	All
Application	Libtiff	Libtiff	4.0.1	All	All	All
Application	Libtiff	Libtiff	4.0.2	All	All	All
Application	Libtiff	Libtiff	3.4	All	All	All
Application	Libtiff	Libtiff	3.4	beta18	All	All
Application	Libtiff	Libtiff	3.4	beta24	All	All
Application	Libtiff	Libtiff	3.4	beta28	All	All
Application	Libtiff	Libtiff	3.4	beta29	All	All
Application	Libtiff	Libtiff	3.4	beta31	All	All
Application	Libtiff	Libtiff	3.4	beta32	All	All
Application	Libtiff	Libtiff	3.4	beta34	All	All
Application	Libtiff	Libtiff	3.4	beta35	All	All
Application	Libtiff	Libtiff	3.4	beta36	All	All
Application	Libtiff	Libtiff	3.4	beta37	All	All
Application	Libtiff	Libtiff	3.5.1	All	All	All
Application	Libtiff	Libtiff	3.5.2	All	All	All
Application	Libtiff	Libtiff	3.5.3	All	All	All
Application	Libtiff	Libtiff	3.5.4	All	All	All
Application	Libtiff	Libtiff	3.5.5	All	All	All
Application	Libtiff	Libtiff	3.5.6	All	All	All
Application	Libtiff	Libtiff	3.5.6	beta	All	All
Application	Libtiff	Libtiff	3.5.7	All	All	All
Application	Libtiff	Libtiff	3.5.7	alpha	All	All
Application	Libtiff	Libtiff	3.5.7	alpha2	All	All
Application	Libtiff	Libtiff	3.5.7	alpha3	All	All
Application	Libtiff	Libtiff	3.5.7	alpha4	All	All
Application	Libtiff	Libtiff	3.5.7	beta	All	All
Application	Libtiff	Libtiff	3.6.0	All	All	All

Application	Libtiff	Libtiff	3.6.0	beta	All	All
Application	Libtiff	Libtiff	3.6.0	beta2	All	All
Application	Libtiff	Libtiff	3.6.1	All	All	All
Application	Libtiff	Libtiff	3.7.0	All	All	All
Application	Libtiff	Libtiff	3.7.0	alpha	All	All
Application	Libtiff	Libtiff	3.7.0	beta	All	All
Application	Libtiff	Libtiff	3.7.0	beta2	All	All
Application	Libtiff	Libtiff	3.7.1	All	All	All
Application	Libtiff	Libtiff	3.7.2	All	All	All
Application	Libtiff	Libtiff	3.7.3	All	All	All
Application	Libtiff	Libtiff	3.7.4	All	All	All
Application	Libtiff	Libtiff	3.8.0	All	All	All
Application	Libtiff	Libtiff	3.8.1	All	All	All
Application	Libtiff	Libtiff	3.8.2	All	All	All
Application	Libtiff	Libtiff	3.9	All	All	All
Application	Libtiff	Libtiff	3.9.0	All	All	All
Application	Libtiff	Libtiff	3.9.0	beta	All	All
Application	Libtiff	Libtiff	3.9.1	All	All	All
Application	Libtiff	Libtiff	3.9.2	All	All	All
Application	Libtiff	Libtiff	3.9.2-5.2.1	All	All	All
Application	Libtiff	Libtiff	3.9.3	All	All	All
Application	Libtiff	Libtiff	3.9.4	All	All	All
Application	Libtiff	Libtiff	3.9.5	All	All	All
Application	Libtiff	Libtiff	4.0	All	All	All
Application	Libtiff	Libtiff	4.0	alpha	All	All
Application	Libtiff	Libtiff	4.0	beta1	All	All
Application	Libtiff	Libtiff	4.0	beta2	All	All
Application	Libtiff	Libtiff	4.0	beta3	All	All
Application	Libtiff	Libtiff	4.0	beta4	All	All
Application	Libtiff	Libtiff	4.0	beta5	All	All
Application	Libtiff	Libtiff	4.0	beta6	All	All
Application	Libtiff	Libtiff	4.0.1	All	All	All
Application	Libtiff	Libtiff	4.0.2	All	All	All
Application	Libtiff	Libtiff	All	All	All	All

Reference	Source	Link
Malformed Request	BID	www.securityfocus.com/bid
libTIFF: Multiple vulnerabilities (GLSA 201701-16) — Gentoo Security	GENTOO	security.gentoo.org
Debian -- Security Information -- DSA-2744-1 tiff	DEBIAN	www.debian.org
996052 – (CVE-2013-4243) CVE-2013-4243 libtiff (gif2tiff): possible heap-based buffer overflow in readgifimage()	CONFIRM	bugzilla.redhat.com/show_bug.cgi?id=996052
Bug 2451 – CVE-2013-4243 libtiff (gif2tiff): possible heap-based buffer overflow in readgifimage()	CONFIRM	bugzilla.mozilla.org/show_bug.cgi?id=2451
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Security Advisory SA54543 - Debian update for tiff - Secunia	SECUNIA	secunia.com
About Secunia Research Flexera	SECUNIA	secunia.com
access.redhat.com CVE-2013-4243	MISC	access.redhat.com
Red Hat Customer Portal	MISC	access.redhat.com
Red Hat Customer Portal	MISC	access.redhat.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.

Legacy QID Mappings

[710479](#) Gentoo Linux libTIFF Multiple Vulnerabilities (GLSA 201701-16)

© 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