



CVE-2011-1167

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

Summary

CVE	CVE-2011-1167
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-28 16:55:00 UTC
Updated	2023-02-13 01:19:00 UTC
Description	Heap-based buffer overflow in the thunder (aka ThunderScan) decoder in tif_thunder.c in LibTIFF 3.9.4 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (crash) via crafted TIFF image data.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	3.4	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	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	All	All	All	All

References						
Reference						Source
Zero Day Initiative						MISC
Ubuntu update for tiff - Secunia.com						SECUNIA
APPLE-SA-2012-02-01-1 OS X Lion v10.7.3 and Security Update 2012-001						APPLE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
Red Hat update for libtiff - Secunia.com						SECUNIA
The Slackware Linux Project: Slackware Security Advisories						SLACKWARE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:009						SUSE
KB27244-Vulnerabilities in BlackBerry Enterprise Server components that process images could allow remote code execution						CONFIRM
LibTIFF Buffer Overflow in ThunderCode Decoder Lets Remote Users Execute Arbitrary Code - SecurityTracker						SECTRAK
Libtiff ThunderCode Decoder THUNDER_2BITDELTAS Remote Code Execution Vulnerability - CXSecurity.com						SREASON
Security Advisory SA50726 - Gentoo update for tiff - Secunia						SECUNIA
Fedora update for libtiff - Secunia.com						SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
APPLE-SA-2012-09-19-1 iOS 6						APPLE
[SECURITY] Fedora 13 Update: libtiff-3.9.4-4.fc13						FEDORA
684939 – (CVE-2011-1167) CVE-2011-1167 libtiff: heap-based buffer overflow in thunder decoder (ZDI-11-107)						CONFIRM
About the security content of OS X Lion v10.7.4 and Security Update 2012-002						CONFIRM
SecurityFocus						BUGTRAQ
APPLE-SA-2012-05-09-1 OS X Lion v10.7.4 and Security Update 2012-002						APPLE
USN-1102-1: tiff vulnerability Ubuntu						UBUNTU
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
Red Hat Customer Portal						MISC
About the security content of OS X Lion v10.7.3 and Security Update 2012-001						CONFIRM
Debian -- Security Information -- DSA-2210-1 tiff						DEBIAN
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
access.redhat.com CVE-2011-1167						MISC

Support	REDHAT
Debian update for tiff - Secunia.com	SECUNIA
libTIFF ThunderCode Decoder Heap Buffer Overflow Vulnerability	BID
[SECURITY] Fedora 14 Update: libtiff-3.9.4-4.fc14	FEDORA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Support / Security / Advisories // MDVSA-2011:064 Mandriva	MANDRIVA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Slackware update for libtiff - Secunia.com	SECUNIA
IBM X-Force Exchange	XF
Gentoo Linux Documentation -- libTIFF: Multiple vulnerabilities	GENTOO
71256	OSVDB
Bug 2300 – Thunder Decoder Vulnerability	CONFIRM
About the security content of iOS 6	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)