CVE-2009-5022

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-5022
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-03 20:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Heap-based buffer overflow in tif_ojpeg.c in the OJPEG decoder in LibTIFF before 3.9.5 allows remote attackers to execute

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

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	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
LibTIFF Heap Overflow in OJPEG Decoder Lets Remote User's Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da
Bug 1999 – OJPEG Crash, Pointer Overwritten during decode	af854a3a-2127-422b-91ae-364da
oss-security - libtiff CVE assignments	af854a3a-2127-422b-91ae-364da
Fedora update for libtiff - Secunia.com	af854a3a-2127-422b-91ae-364da
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da
Changes in TIFF v3.9.5	af854a3a-2127-422b-91ae-364da
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da
USN-1120-1: tiff vulnerability | Ubuntu	af854a3a-2127-422b-91ae-364da
Support	af854a3a-2127-422b-91ae-364da
Support / Security / Advisories / / MDVSA-2011:078 | Mandriva	af854a3a-2127-422b-91ae-364da
695885 – (CVE-2009-5022) CVE-2009-5022 libtiff ojpeg buffer overflow	af854a3a-2127-422b-91ae-364da
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da
Malformed Request	af854a3a-2127-422b-91ae-364da
[SECURITY] Fedora 14 Update: libtiff-3.9.5-1.fc14	af854a3a-2127-422b-91ae-364da
Security Advisory SA50726 - Gentoo update for tiff - Secunia	af854a3a-2127-422b-91ae-364da
Gentoo Linux Documentation -- libTIFF: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da
Debian -- Security Information -- DSA-2256-1 tiff	af854a3a-2127-422b-91ae-364da
Red Hat Customer Portal	MITRE
CVE-2009-5022 - Red Hat Customer Portal	MITRE

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.