Libtiff: libtiff write-what-where

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

Summary

CVE	CVE-2025-9900
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-23 17:15:38 UTC
Updated	2026-04-20 22:16:22 UTC
Description	A flaw was found in Libtiff. This vulnerability is a "write-what-where" condition, triggered when the library processes a specia

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from secalert@redhat.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.000360000 probability, percentile 0.106500000 (date 2026-04-20)

Problem Types: CWE-123 | CWE-123 Write-what-where Condition

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:4.6.0-6.el10_0.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:4.6.0-6.el10_1.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:3.9.4-12.el7_9.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:4.0.3-35.el7_9.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.9.4-14.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:4.0.9-35.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:4.0.9-3.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:3.9.4-13.el8_2.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:4.0.9-17.el8_2.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:8.10-3.el8_2.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:3.9.4-13.el8_4.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:4.0.9-18.el8_4.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:8.10-3.el8_4.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:3.9.4-13.el8_4.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:4.0.9-18.el8_4.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:8.10-3.el8_4.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:3.9.4-13.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:4.0.9-21.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:8.10-3.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:3.9.4-13.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:4.0.9-21.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:8.10-3.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:3.9.4-13.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:4.0.9-21.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:8.10-3.el8_6.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:3.9.4-13.el8_8.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:4.0.9-29.el8_8.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:8.10-3.el8_8.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:3.9.4-13.el8_8.1 * rpm

CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:4.0.9-29.el8_8.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:8.10-3.el8_8.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:4.4.0-13.el9_6.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:4.4.0-15.el9_7.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:4.2.0-3.el9_0.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:4.4.0-8.el9_2.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:4.4.0-12.el9_4.4 * rpm
CNA	Red Hat	Red Hat AI Inference Server 3.2	unaffected sha256:bddcf7ab6d576572b6d6
CNA	Red Hat	Red Hat AI Inference Server 3.2	unaffected sha256:7856bdb7ae0d643a7b9
CNA	Red Hat	Red Hat AI Inference Server 3.2	unaffected sha256:14e32e88f1b89f59ed34
CNA	Red Hat	Red Hat AI Inference Server 3.2	unaffected sha256:dcb9d1cd005c40b6db6f
CNA	Red Hat	Red Hat AI Inference Server 3.2	unaffected sha256:53007894763e03f609c3
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:310df392f638ef6eca1a2
CNA	Red Hat	Red Hat Hardened Images	unaffected 4.7.1-2.1.hum1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified

References

Reference	Source	Link	Tag
access.redhat.com/errata/RHSA-2026:7504	secalert@redhat.com	access.redhat.com	
libtiff.gitlab.io/libtiff/releases/v4.7.1.html	secalert@redhat.com	libtiff.gitlab.io	
access.redhat.com/errata/RHSA-2026:0001	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:20998	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:17675	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:17739	secalert@redhat.com	access.redhat.com	
gitlab.com/libtiff/libtiff/-/merge_requests/732	secalert@redhat.com	gitlab.com	
access.redhat.com/errata/RHSA-2025:23080	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0077	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:23079	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:20956	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:17738	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19947	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21994	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:23078	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21407	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2025/09/26/3	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	

access.redhat.com/errata/RHSA-2025:19276	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21060	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3461	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:17710	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0078	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21061	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:17651	secalert@redhat.com	access.redhat.com	
lists.debian.org/debian-lts-announce/2025/09/msg00031.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
access.redhat.com/errata/RHSA-2026:3462	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21508	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2025:21507	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21062	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19113	secalert@redhat.com	access.redhat.com	
github.com/SexyShoelessGodofWar/LibTiff-4.7.0-Write-What-Where	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	
gitlab.com/libtiff/libtiff/-/issues/704	secalert@redhat.com	gitlab.com	
access.redhat.com/errata/RHSA-2025:17740	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19156	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2025-9900	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0076	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19906	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21506	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Gareth C (AnchorSec Ltd.) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-09-03T02:48:12.111Z	Reported to Red Hat.
CNA	2025-09-22T14:29:35.767Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not

meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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