Libtiff: libtiff: arbitrary code execution or denial of service via signed integer overflow in tiff file processing

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

Summary

CVE	CVE-2026-4775
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-24 15:16:39 UTC
Updated	2026-04-21 16:34:57 UTC
Description	A flaw was found in the libtiff library. A remote attacker could exploit a signed integer overflow vulnerability in the putcontig8

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from secalert@redhat.com

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

EPSS: 0.000330000 probability, percentile 0.094620000 (date 2026-04-21)

Problem Types: CWE-190 | CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Libtiff	Libtiff	-	All	All	All
Operating System	Redhat	Enterprise Linux	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Hardened Images	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat Hardened Images	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2026-4775	secalert@redhat.com	access.redhat.com	Third Party
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Trac
lists.debian.org/debian-lts-announce/2026/04/msg00016.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Mailing Lis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank PrymEvol and Quang Luong for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-24T14:23:23.826Z	Reported to Red Hat.
CNA	2026-03-24T14:33:35.730Z	Made public.

Workarounds

CNA: To mitigate this issue, avoid processing untrusted or maliciously crafted TIFF files with applications linked against the libtiff library. If processing untrusted TIFF files is unavoidable, consider running the affected applications within a sandboxed environment to limit the potential impact of successful exploitation. This operational control helps contain the effects of an out-of-bounds write, reducing the risk of denial of service or arbitrary code execution.

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