Libcap: libcap: privilege escalation via toctou race condition in cap_set_file()

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

Summary

CVE	CVE-2026-4878
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 16:16:31 UTC
Updated	2026-04-25 02:16:03 UTC
Description	A flaw was found in libcap. A local unprivileged user can exploit a Time-of-check-to-time-of-use (TOCTOU) race condition ir

Risk And Classification

Primary CVSS: v3.1 6.7 MEDIUM from secalert@redhat.com

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

EPSS: 0.000110000 probability, percentile 0.013320000 (date 2026-04-15)

Problem Types: CWE-367 | CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	6.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Hardened Images	unaffected 2.78-1.1.hum1 * rpm	Not specified
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 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 9	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:7473	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2026/04/07/14	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
www.openwall.com/lists/oss-security/2026/04/07/4	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
www.openwall.com/lists/oss-security/2026/04/09/6	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
access.redhat.com/security/cve/CVE-2026-4878	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2026/04/09/5	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
www.openwall.com/lists/oss-security/2026/04/08/9	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Ali Raza for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-26T06:56:21.213Z	Reported to Red Hat.
CNA	2026-04-06T00:00:00.000Z	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.