



# Libcap: libcap: privilege escalation via toctou race condition in cap\_set\_file()

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

## Summary

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

## 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

Integrity

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

© [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](#)