Bug 2451615 (CVE-2026-4878) - CVE-2026-4878 libcap: libcap: Privilege escalation via TOCTOU race condition in cap_set_file()

Keywords: Security

Status: NEW

Alias: CVE-2026-4878

Deadline: 2026-04-06

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-26 06:56 UTC by OSIDB Bzimport

Modified: 2026-05-04 01:38 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2026:13279	0	None	None	None	2026-05-04 01:03:01 UTC
Red Hat Product Errata	RHSA-2026:12423	0	None	None	None	2026-04-30 17:40:36 UTC
Red Hat	RHSA-2026:12441	0	None	None	None	2026-04-30

Product Errata						18:47:27 UTC
Red Hat Product Errata	RHSA-2026:13285	0	None	None	None	2026-05-04 01:38:11 UTC

OSIDB Bzimport 2026-03-26 06:56:43 UTC Description

A time-of-check-to-time-of-use (TOCTOU) race condition in libcap’s cap_set_file() allows a local unprivileged user to redirect file capability updates to an attacker-controlled file and gain elevated privileges. The function first validates the target path with lstat() (which does not follow symlinks) and enforces that it is a regular, non-symlink file, but then applies or removes security.capability using setxattr() / removexattr(), which re-resolve the path and do follow symlinks. An attacker with write access to the parent directory can exploit the window between these calls by atomically swapping the validated regular file with a symlink or alternate file using renameat2(RENAME_EXCHANGE). As a result, capabilities can be injected into or stripped from an unintended executable, for example when a privileged process (such as setcap, package scripts, or container tooling) invokes cap_set_file() on an attacker-influenced path. This can be abused to grant capabilities like CAP_SETUID to an attacker’s binary and escalate to root.

errata-xmlrpc 2026-04-30 17:40:30 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2026:12423 https://access.redhat.com/errata/RHSA-2026:12423

errata-xmlrpc 2026-04-30 18:47:26 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2026:12441 https://access.redhat.com/errata/RHSA-2026:12441

errata-xmlrpc 2026-05-04 01:38:10 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2026:13285 https://access.redhat.com/errata/RHSA-2026:13285

Note

You need to log in before you can comment on or make changes to this bug.