



Bug 2453813 (CVE-2026-35091) - CVE-2026-35091 corosync: Corosync: Denial of Service and information disclosure via crafted UDP packet

Keywords: Security ✕

Reported: 2026-04-01 11:31 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-05-05 10:23 UTC ([History](#))

Alias: CVE-2026-35091

CC List: 1 user ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: [2453815](#)


Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments	(Terms of Use)
--------------------	--------------------------------

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2026:13644	0	None	None	None	2026-05-05 09:18:44 UTC
Red Hat Product Errata	RHSA-2026:13657	0	None	None	None	2026-05-05 10:04:51 UTC
Red Hat Product Errata	RHSA-2026:13673	0	None	None	None	2026-05-05 10:23:47 UTC

OSIDB Bzimport  2026-04-01 11:31:24 UTC[Description](#)

Wrong return value vulnerability in the Corosync membership commit token sanity check in exec/totemsrc.c. The flaw occurs in `check_memb_commit_token_sanity()` where truncated messages (`msg_len < sizeof(struct memb_commit_token)`) incorrectly return `0` (success) instead of `-1` (failure). As a result, `message_handler_memb_commit_token()` continues processing attacker-controlled, undersized input, performs an allocation based on the short length, and then accesses struct `memb_commit_token` fields beyond the allocated region, triggering an out-of-bounds read (ASAN-confirmed). This can be exploited remotely without authentication in `totemudp/totemudpu` mode by sending a single crafted UDP packet to the Corosync port (default 5405), causing a denial of service and potentially leaking limited memory contents.

errata-xmlrpc 2026-05-05 09:18:44 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10

Via RHSA-2026:13644 <https://access.redhat.com/errata/RHSA-2026:13644>

errata-xmlrpc 2026-05-05 10:04:50 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2026:13657 <https://access.redhat.com/errata/RHSA-2026:13657>

errata-xmlrpc 2026-05-05 10:23:46 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2026:13673 <https://access.redhat.com/errata/RHSA-2026:13673>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

