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

Keywords: Security

Status: NEW

Alias: CVE-2026-35091

Product: Security Response

Component: vulnerability

Version: unspecified

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

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

Modified: 2026-04-06 07:27 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-01 11:31:24 UTC Description

```
Wrong return value vulnerability in the Corosync membership
commit token sanity check in exec/totemsrp.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.

Note

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