Bug 2453814 (CVE-2026-35092) - CVE-2026-35092 corosync: Corosync: Denial of Service via integer overflow in join message validation

Keywords: Security

Status: NEW

Alias: CVE-2026-35092

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: ~~2453821~~

Blocks:

TreeView+ depends on / blocked

Reported: 2026-04-01 11:32 UTC by OSIDB Bzimport

Modified: 2026-05-05 10:23 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	RHSA-2026:13644	0	None	None	None	2026-05-05 09:18:47 UTC
Red Hat Product Errata	RHSA-2026:13657	0	None	None	None	2026-05-05 10:04:52 UTC
Red Hat Product Errata	RHSA-2026:13673	0	None	None	None	2026-05-05 10:23:47 UTC

OSIDB Bzimport 2026-04-01 11:32:27 UTC Description

Integer overflow (wraparound) vulnerability in Corosync’s join message sanity validation in exec/totemsrp.c. The flaw is in check_memb_join_sanity(), where proc_list_entries and failed_list_entries are attacker-controlled 32-bit unsigned values received from the network and are added together before being promoted to size_t. This allows the addition (proc_list_entries + failed_list_entries) to wrap around in 32-bit arithmetic (e.g., 0x80000000 + 0x80000000 = 0), causing required_len to be calculated too small and allowing a short packet to pass validation. As a result, Corosync proceeds with processing malformed input that should have been rejected, which can be exploited remotely without authentication in totemudp/totemudpu mode via crafted UDP packets to crash the service, resulting in a denial of service.

errata-xmlrpc 2026-05-05 09:18:46 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 10:04:51 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.