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: 2026-05-06 16:30 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 09:18:44 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

Red Hat Product Errata	RHSA-2026:14205	0	None	None	None	2026-05-06 15:47:19 UTC
Red Hat Product Errata	RHSA-2026:14210	0	None	None	None	2026-05-06 16:15:29 UTC
Red Hat Product Errata	RHSA-2026:14211	0	None	None	None	2026-05-06 16:10:45 UTC
Red Hat Product Errata	RHSA-2026:14212	0	None	None	None	2026-05-06 16:27:52 UTC
Red Hat Product Errata	RHSA-2026:14213	0	None	None	None	2026-05-06 16:30:23 UTC
Red Hat Product Errata	RHSA-2026:14214	0	None	None	None	2026-05-06 16:20:07 UTC
Red Hat Product Errata	RHSA-2026:14215	0	None	None	None	2026-05-06 16:15:05 UTC
Red Hat Product Errata	RHSA-2026:14216	0	None	None	None	2026-05-06 16:25:55 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/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.
```

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

errata-xmlrpc 2026-05-06 15:47:18 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10.0 Extended Update Support

Via RHSA-2026:14205 https://access.redhat.com/errata/RHSA-2026:14205

errata-xmlrpc 2026-05-06 16:10:44 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2026:14211 https://access.redhat.com/errata/RHSA-2026:14211

errata-xmlrpc 2026-05-06 16:15:04 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On

Via RHSA-2026:14215 https://access.redhat.com/errata/RHSA-2026:14215

errata-xmlrpc 2026-05-06 16:15:27 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2026:14210 https://access.redhat.com/errata/RHSA-2026:14210

errata-xmlrpc 2026-05-06 16:20:05 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2026:14214 https://access.redhat.com/errata/RHSA-2026:14214

errata-xmlrpc 2026-05-06 16:25:54 UTC Comment 10

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.8 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.8 Telecommunications Update Service

Via RHSA-2026:14216 https://access.redhat.com/errata/RHSA-2026:14216

errata-xmlrpc 2026-05-06 16:27:51 UTC Comment 11

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2026:14212 https://access.redhat.com/errata/RHSA-2026:14212

errata-xmlrpc 2026-05-06 16:30:22 UTC Comment 12

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.6 Extended Update Support

Via RHSA-2026:14213 https://access.redhat.com/errata/RHSA-2026:14213

Note

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