Bug 2453169 - corosync: pre-auth OOB read in check_memb_commit_token_sanity + integer overflow in check_memb_join_sanity

Keywords: Regression × Security ×

Status: NEW

Alias: None

Product: Fedora

Component: corosync

Version: rawhide

Hardware: All

OS: Linux

Priority: unspecified

Severity: high

Target Milestone: ---

Assignee: Jan Friesse

QA Contact: Fedora Extras Quality Assurance

Docs Contact:

URL: https://github.com/corosync/corosync/...

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-30 20:18 UTC by Sebastian Alba

Modified: 2026-03-30 20:21 UTC (History)

CC List: 3 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Type: ---

Embargoed:

Dependent Products:

Attachments	(Terms of Use)	
PoC for Bug 1: ASAN heap-buffer-overflow in check_memb_commit_token_sanity (2.70 KB, text/x-csrc) 2026-03-30 20:20 UTC, Sebastian Alba	*no flags*	Details
Integer overflow bypass in check_memb_join_sanity (4.68 KB, text/x-csrc) 2026-03-30 20:20 UTC, Sebastian Alba	*no flags*	Details
ASAN output confirming OOB read (2.45 KB, text/plain) 2026-03-30 20:21 UTC, Sebastian Alba	*no flags*	Details
Output confirming integer overflow (1.03 KB, text/plain) 2026-03-30 20:21 UTC, Sebastian Alba	*no flags*	Details
		View All

Sebastian Alba 2026-03-30 20:18:21 UTC Description

Two vulnerabilities in exec/totemsrp.c (current HEAD commit ee28d8f). Both pre-auth in totemudp/totemudpu mode. Different from CVE-2025-30472.

BUG 1 - CWE-393: check_memb_commit_token_sanity() returns 0 instead of -1 when msg_len < sizeof(struct memb_commit_token). Compare with check_orf_token_sanity() which correctly returns -1. This allows message_handler_memb_commit_token() to process a truncated message causing heap-buffer-overflow READ. ASAN confirmed. Fix: change return (0) to return (-1) at ~line 3814.

~~BUG 2~~ - CWE-190: In check_memb_join_sanity() ~line 3789, (proc_list_entries + failed_list_entries) wraps in uint32 before size_t promotion. With proc=0x80000000 + failed=0x80000000, sum=0, bypassing bounds check. Fix: cast to size_t before addition.

ASAN harnesses will be attached after submission.

Reproducible: Always

Steps to Reproduce:
1. gcc -fsanitize=address,undefined -g -O0 harness_bug1_minimal.c -o harness_bug1
2. ./harness_bug1
3. Observe ASAN heap-buffer-overflow READ
Actual Results:
ASAN reports heap-buffer-overflow READ of size 4, 21 bytes past allocation

Expected Results:
check_memb_commit_token_sanity should return -1 and reject the short message

Additional Information:
Reporter: Sebastian Alba Vives (@Sebasteuo / 0xS4bb1)
Contact: sebasjosue84
90-day disclosure deadline: June 28, 2026.
Requesting separate CVE assignments for each vulnerability.
Also reported to jfriesse and secalert.
CVSS Bug 1: 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H)
CVSS ~~Bug 2~~: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Sebastian Alba 2026-03-30 20:20:21 UTC Comment 1

Created attachment 2135489 [details]
PoC for Bug 1: ASAN heap-buffer-overflow in check_memb_commit_token_sanity

Sebastian Alba 2026-03-30 20:20:42 UTC Comment 2

Created attachment 2135490 [details]
Integer overflow bypass in check_memb_join_sanity

Sebastian Alba 2026-03-30 20:21:01 UTC Comment 3

Created attachment 2135491 [details]
ASAN output confirming OOB read

Sebastian Alba 2026-03-30 20:21:16 UTC Comment 4

Created attachment 2135493 [details]
Output confirming integer overflow

Note

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