

Report

Cybersecurity Advisory for C-Open

Attachments

Contents

1 Overview	2
2 Affected Versions	2
3 Vulnerability Details	2
3.1 CVE-2026-82357	2
3.2 CVE-2026-82358	3
4 Mitigation Steps	4
5 Acknowledgements	4
6 Additional Information	4

1 Overview

This advisory addresses cybersecurity vulnerabilities discovered in the C-Open CANopen stack. The vulnerabilities may allow denial of service and unauthorized write access to read-only objects, and require immediate action to mitigate potential exploitation.

C-Open devices located on networks that are isolated from potential attackers, such as internal CAN networks or those protected by proper network segmentation, have reduced exposure to the identified threats.

2 Affected Versions

- C-Open versions prior to 1.1.1

3 Vulnerability Details

3.1 CVE-2026-82357

CVE ID	CVE-2026-82357
Description	NULL pointer dereference in LSS inquire-identity handler
Impact	Denial of service
Exploitability	This vulnerability can be exploited by a CAN-bus-local attacker capable of sending LSS packets to a CANopen device using the C-Open library. The attacker must have access to the CAN bus segment.
CVSS v3.1 Base Score	6.5
CVSS v3.1 Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE	CWE-476: NULL Pointer Dereference
Recommendation	Upgrade to C-Open version 1.1.1 or later

Technical Details:

The LSS implementation in `co_lss_inquire_identity()` assumed that calls to `co_entry_find()` for object 0x1018 (Identity Object) would always succeed. However, if the user-defined object dictionary does not contain all required subindexes (1-4), `co_entry_find()` returns NULL. The code then passed this NULL pointer to `co_od_get_value()`, which dereferenced `entry->data` without checking, causing a NULL pointer dereference at `co_od.c:156`.

The vulnerability can be triggered by sending two unauthenticated LSS frames:

1. CS_SWITCH_GLOBAL to enter CONFIG state
2. CS_INQUIRE_IDENTITY for a missing subindex

Fix:

The fix includes multiple defensive measures:

- Added assertions in `co_lss_init()` to verify that object 0x1018 and all required subindexes (1-4) exist at startup
- Modified `co_lss_identity_get()` to check if `co_entry_find()` returns NULL and return UINT32_MAX as a safe default value
- Added command validation in `co_lss_inquire_identity()` to reject invalid command codes

3.2 CVE-2026-82358

CVE ID	CVE-2026-82358
Description	Write-protection bypass in SDO segmented transfer
Impact	Unauthorized write access to read-only objects, Data integrity violation
Exploitability	This vulnerability can be exploited by a CAN-bus-local attacker capable of sending malicious SDO packets to a CANopen device using the C-Open library. The attacker must have access to the CAN bus segment.
CVSS v3.1 Base Score	6.5
CVSS v3.1 Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE	CWE-863: Incorrect Authorization
Recommendation	Upgrade to C-Open version 1.1.1 or later

Technical Details:

The SDO server's segmented upload and download handlers (`co_sdo_rx_upload_seg_req()` and `co_sdo_rx_download_seg_req()`) did not verify that a valid segmented transfer job was in progress before processing segment frames. This allowed an attacker to bypass write-protection checks by:

1. Sending an SDO upload-init request for a read-only object (which sets `job->sdo.data` to point to the object's storage)
2. Sending SDO download-segment frames to write arbitrary data to that read-only object's memory

The download-init handler correctly checks the OD_WRITE permission flag and rejects writes to read-only objects. However, the segmented transfer handlers assumed a prior init had already validated permissions and did not re-check the job type.

Fix:

Added job type validation in both segmented transfer handlers:

- `co_sdo_rx_upload_seg_req()` now checks `job->type == CO_JOB_SDO_UPLOAD`
- `co_sdo_rx_download_seg_req()` now checks `job->type == CO_JOB_SDO_DOWNLOAD`

If the job type is incorrect, the handlers abort with `CO_SDO_ABORT_ACCESS` instead of processing the segment.

4 Mitigation Steps

Affected users are advised to upgrade to C-Open version 1.1.1 or later to mitigate identified vulnerabilities.

As an alternative measure and to enhance security, ensure that C-Open devices are not connected to untrusted networks. Devices that are not accessible to attackers, such as those on isolated networks or protected by proper network segmentation and access controls, have reduced exposure to potential threats.

Additionally, for CVE-2026-82358, ensure that the Identity Object (0x1018) in your object dictionary contains all four required subindexes (vendor ID, product code, revision number, and serial number) as specified by the CANopen standard.

5 Acknowledgements

We acknowledge the efforts of f0rw4rd from quellsec.dev who identified and reported these vulnerabilities.

6 Additional Information

For further inquiries or support, please contact:

- **Support Contact:** support@rt-labs.com
- **Website:** <https://rt-labs.com>
- **Security Information:** <https://rt-labs.com/cyber-security/>

Disclaimer: This advisory is provided for informational purposes only. RT-Labs is not liable for any damage caused by the exploitation of the vulnerabilities listed.