

# Report

## Cybersecurity Advisory for SOEM

Attachments

## Contents

|                                 |          |
|---------------------------------|----------|
| <b>1 Overview</b>               | <b>2</b> |
| <b>2 Affected Versions</b>      | <b>2</b> |
| <b>3 Vulnerability Details</b>  | <b>2</b> |
| 3.1 CVE-2026-70388 . . . . .    | 2        |
| 3.2 CVE-2026-82943 . . . . .    | 3        |
| 3.3 CVE-2026-82944 . . . . .    | 4        |
| 3.4 CVE-2026-82945 . . . . .    | 5        |
| 3.5 CVE-2026-82946 . . . . .    | 6        |
| 3.6 CVE-2026-82947 . . . . .    | 6        |
| <b>4 Mitigation Steps</b>       | <b>7</b> |
| <b>5 Additional Information</b> | <b>8</b> |

## 1 Overview

This advisory covers several security vulnerabilities in SOEM (Simple Open EtherCAT Master) versions up to and including 2.0.0. All vulnerabilities can be triggered by a malicious or compromised device on the same EtherCAT network.

## 2 Affected Versions

- SOEM versions prior to 2.0.1

## 3 Vulnerability Details

### 3.1 CVE-2026-70388

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE ID</b>      | CVE-2026-70388                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Title</b>       | Memory Corruption via Integer Underflow in Message Length Validation                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | SOEM version 2.0.0 and earlier contains vulnerabilities where a malicious device on the network can send specially crafted messages that cause the master to write data outside allocated memory boundaries. The software performs arithmetic on message length values without proper validation, allowing negative or extremely large values to bypass safety checks. This can corrupt memory and potentially allow an attacker to execute arbitrary code on the master system. |
| <b>CWE</b>         | CWE-191 (Integer Underflow (Wrap or Wraparound)), CWE-195 (Signed to Unsigned Conversion Error), CWE-787 (Out-of- bounds Write)                                                                                                                                                                                                                                                                                                                                                  |

|                             |                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Impact</b>               | Memory corruption; potential crash or code execution on the master                                                                        |
| <b>Exploitability</b>       | This vulnerability can be exploited by a malicious EtherCAT device that implements the SoE, CoE, EoE or FoE protocols.                    |
| <b>CVSS v3.1 Base Score</b> | 8.3 (High)                                                                                                                                |
| <b>CVSS v3.1 Vector</b>     | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H                                                                                              |
| <b>Recommendation</b>       | Upgrade to SOEM version 2.0.1 or later                                                                                                    |
| <b>Reported by</b>          | f0rw4rd (quellsec.dev), alosafuzz, 3ntr0py1337 (LeetProtect Research), Brian Willows (graith.co.uk), Eun0us (EpsilonOrg), Mayur Agnihotri |

### Technical Details

The SoE, CoE, EoE and FoE message handlers compute a payload size by subtracting a fixed header size from the slave-supplied length field using signed arithmetic. When the slave reports a length smaller than the header, the result is a large negative number. The negative value is used in a memory copy, where it is treated as a huge positive size (approximately  $2^{63}$  bytes), writing far past the destination buffer.

### Fix

A validation step was added inside the central mailbox receive function. It now checks every incoming message's length against the per-protocol minimum and against the physical mailbox size before handing the message to any parser. A message that fails either check is discarded.

## 3.2 CVE-2026-82943

|                             |                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE ID</b>               | CVE-2026-82943                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Title</b>                | Out-of-Bounds Read via Unchecked Length Values                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>          | SOEM version 2.0.0 and earlier contains vulnerabilities where a malicious device can send messages that cause the master to read data from memory locations beyond the intended buffer. The software uses length values from device responses without validating them against actual buffer sizes. An attacker can exploit this to extract up to 64KB of data from the master's memory. |
| <b>CWE</b>                  | CWE-125 (Out-of-bounds Read), CWE-195 (Signed to Unsigned Conversion Error), CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)                                                                                                                                                                                                                                       |
| <b>Impact</b>               | Disclosure of master process memory; potential crash                                                                                                                                                                                                                                                                                                                                    |
| <b>Exploitability</b>       | This vulnerability can be exploited by a malicious EtherCAT device that implements the SoE, CoE, EoE or FoE protocols.                                                                                                                                                                                                                                                                  |
| <b>CVSS v3.1 Base Score</b> | 6.5 (Medium)                                                                                                                                                                                                                                                                                                                                                                            |

---

|                         |                                                                                                                            |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVSS v3.1 Vector</b> | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N                                                                               |
| <b>Recommendation</b>   | Upgrade to SOEM version 2.0.1 or later                                                                                     |
| <b>Reported by</b>      | f0rw4rd (quellsec.dev), alosafuzz, 3ntr0py1337<br>(LeetProtect Research), Brian Willows<br>(graith.co.uk), Mayur Agnihotri |

---

## Technical Details

The FoE, SoE, and CoE message handlers used the slave-supplied length field as the source size for a memory copy, without checking that it fits within the actual received buffer (which is at most 1487 bytes). A slave that claims a large length while sending a short message causes the copy to read past the buffer boundary into adjacent memory, which is then returned to the caller as data. A separate bug in the SoE handler caused an unassigned internal pointer to be used as the copy source after the receive completed, reading from near address zero.

## Fix

The central mailbox receive validation (added for CVE-2026-70388) also limits the slave-supplied length to the physical mailbox capacity, so derived copy sizes are bounded by the actual buffer. The stale pointer issue was fixed by computing the source pointer after the receive returns (patch provided by Sankalp Thakur).

## 3.3 CVE-2026-82944

---

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE ID</b>               | CVE-2026-82944                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Title</b>                | Buffer Overflow in CoE SDO Upload<br>Multi-Segment Data Transfers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>          | SOEM version 2.0.0 and earlier contains a vulnerability in CoE SDO upload multi-segment data transfers where a malicious device can overflow memory buffers. The software checks the total size only once at the beginning, but doesn't track the cumulative size as multiple segments arrive. An attacker can declare a small initial size to pass validation, then send additional segments that exceed the allocated buffer. This allows the attacker to write controlled data beyond buffer boundaries, potentially enabling code execution. |
| <b>CWE</b>                  | CWE-787 (Out-of-bounds Write), CWE-131 (Incorrect Calculation of Buffer Size), CWE-120 (Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'))                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Impact</b>               | Memory corruption; potential crash or code execution on the master                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Exploitability</b>       | This vulnerability can be exploited by a malicious EtherCAT device that implements the CoE protocol and objects larger than the mailbox size.                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>CVSS v3.1 Base Score</b> | 8.8 (High)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>CVSS v3.1 Vector</b>     | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                       |                                                                 |
|-----------------------|-----------------------------------------------------------------|
| <b>Recommendation</b> | Upgrade to SOEM version 2.0.1 or later                          |
| <b>Reported by</b>    | 3ntrOpy1337 (LeetProtect Research), Akhil Koul, Mayur Agnihotri |

#### Technical Details

When a CoE SDO upload spans multiple segments, the master checked the declared total size against the destination buffer only once at the start. It then copied each arriving segment without tracking how much had been written in total. A slave could declare a small total to pass the initial check, then stream segments continuously, writing past the end of the buffer.

#### Fix

The segment loop now tracks the running total and rejects any segment that exceeds the declared size.

### 3.4 CVE-2026-82945

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE ID</b>               | CVE-2026-82945                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Title</b>                | Memory Corruption via FMMU Configuration Table Overflow                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>          | SOEM version 2.0.0 and earlier contains a vulnerability during device configuration where a malicious device can cause memory corruption. The software writes configuration data to a fixed-size array without checking if the array index exceeds its maximum size of EC_MAXFMMU entries. A device presenting more than EC_MAXFMMU configuration blocks can force writes beyond the array boundary, corrupting adjacent memory structures and potentially disrupting subsequent operations. |
| <b>CWE</b>                  | CWE-787 (Out-of-bounds Write), CWE-129 (Improper Validation of Array Index), CWE-120 (Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'))                                                                                                                                                                                                                                                                                                                                |
| <b>Exploitability</b>       | This vulnerability can be exploited by a malicious EtherCAT device capable of writing its own EEPROM contents.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CVSS v3.1 Base Score</b> | 6.5 (High)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>CVSS v3.1 Vector</b>     | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Recommendation</b>       | Upgrade to SOEM version 2.0.1 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Reported by</b>          | f0rw4rd (quellsec.dev), Brian Willows (graith.co.uk)                                                                                                                                                                                                                                                                                                                                                                                                                                         |

#### Technical Details

During slave configuration the master maintains a table of FMMU configuration data with a fixed maximum of EC\_MAXFMMU entries. The table index was incremented without checking the limit, so a slave presenting more than EC\_MAXFMMU distinct regions caused writes past the end of the table into the adjacent mailbox address fields. The corrupted fields then caused subsequent mailbox operations to target wrong addresses

or use incorrect lengths. The information that triggers the overflow comes from the slave's on-chip EEPROM. The issue is reached automatically during scan time, before any operational state.

#### Fix

The table index is now checked against the maximum before each write. Entries beyond the limit are skipped.

### 3.5 CVE-2026-82946

|                             |                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE ID</b>               | CVE-2026-82946                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Title</b>                | Null Pointer Dereference in Mailbox Error Handling                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>          | SOEM version 2.0.0 and earlier contains a vulnerability where a malicious device can crash the master system. When the software receives an error response, it clears an internal pointer but continues processing. If another message arrives before timeout, the software attempts to use the cleared pointer, causing a crash. An attacker can trigger this with a simple sequence of two messages. |
| <b>CWE</b>                  | CWE-476 (NULL Pointer Dereference),<br>CWE-690 (Unchecked Return Value to NULL Pointer Dereference)                                                                                                                                                                                                                                                                                                    |
| <b>Impact</b>               | Denial of service (master crash)                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Exploitability</b>       | This vulnerability can be exploited by a malicious EtherCAT device capable of sending crafted messages.                                                                                                                                                                                                                                                                                                |
| <b>CVSS v3.1 Base Score</b> | 6.5 (Medium)                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>CVSS v3.1 Vector</b>     | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H                                                                                                                                                                                                                                                                                                                                                           |
| <b>Recommendation</b>       | Upgrade to SOEM version 2.0.1 or later                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Reported by</b>          | alosafuzz                                                                                                                                                                                                                                                                                                                                                                                              |

#### Technical Details

When the mailbox receive function gets an error-typed response, it frees the internal buffer and clears the pointer to NULL. The retry loop then continued without acquiring a new buffer first. On the next iteration it passed the NULL pointer to a receive call, causing an immediate crash.

#### Fix

The retry loop now acquires a fresh buffer before each attempt.

### 3.6 CVE-2026-82947

|               |                                                  |
|---------------|--------------------------------------------------|
| <b>CVE ID</b> | CVE-2026-82947                                   |
| <b>Title</b>  | Multiple Out-of-Bounds Reads in Frame Processing |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>          | SOEM version 2.0.0 and earlier contains multiple vulnerabilities in frame processing where a malicious device can cause the master to read data outside allocated buffers. The software uses length and offset values from device messages without validating them against buffer sizes. This can cause the master to access invalid memory locations, potentially disclosing sensitive information or causing crashes. |
| <b>CWE</b>                  | CWE-125 (Out-of-bounds Read), CWE-787 (Out-of-bounds Write), CWE-191 (Integer Underflow (Wrap or Wraparound)), CWE-129 (Improper Validation of Array Index)                                                                                                                                                                                                                                                             |
| <b>Impact</b>               | Disclosure of master process memory; potential crash                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Exploitability</b>       | Any device on the EtherCAT segment; the frame driver issue requires only a single crafted Ethernet frame                                                                                                                                                                                                                                                                                                                |
| <b>CVSS v3.1 Base Score</b> | 7.1 (High)                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>CVSS v3.1 Vector</b>     | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Recommendation</b>       | Upgrade to SOEM version 2.0.1 or later                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Reported by</b>          | f0rw4rd (quellsec.dev), alosafuzz, Brian Willows (graith.co.uk), Mayur Agnihotri                                                                                                                                                                                                                                                                                                                                        |

## Technical Details

In each affected code path, a length or offset value taken from an incoming frame or slave configuration is used directly to determine how much memory to read, without first checking that the value is within the bounds of the actual buffer. In the frame receive path, the offset of the working counter is not validated to be inside the buffer boundaries. In the cyclic mailbox handlers, the size used to read from and write to the slave's mailbox is taken from a slave-supplied configuration value without limiting it to the available buffer size. A slave that reports an oversized mailbox causes the read or write to extend into adjacent memory. This affects only applications that use the cyclic mailbox mode. In the EoE recv path, timestamp handling assumes buffer is large enough to contain a timestamp.

## Fix

Each path was corrected by validating the relevant value against the actual buffer size before use. Frames or fragments that fail validation are discarded.

## 4 Mitigation Steps

Upgrade to SOEM 2.0.1 or later. All vulnerabilities are fixed in that release. As an alternative measure and to enhance security, ensure that EtherCAT devices are not connected to public networks. Devices that are not accessible to attackers, such as those on isolated networks or protected by firewalls, are at significantly reduced risk.

## 5 Additional Information

For further inquiries or support, please contact:

- **Support Contact:** [support@rt-labs.com](mailto:support@rt-labs.com)
- **Website:** <https://www.rt-labs.com>

**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.