



ESPILON
SECURITY RESEARCH

COORDINATED DISCLOSURE

Out-of-bounds write via integer underflow in SOEM's EtherCAT mailbox parser

CVE-2026-70388

CVSS 8.3 · HIGH

RT-Labs · SOEM EtherCAT master

CVE PUBLISHED 26 Oct 2026

Marouane El Moufid (Eun0us) · shared credit

espilon.net · Association loi 1901 · France



01 Vulnerability

8.3

CVSS 3.1 BASE SCORE · ENISA (CNA)

AV:A / AC:L / PR:N / UI:N / S:U / C:L / I:H / A:H

HIGH

CVE	CVE-2026-70388
Component	SOEM (Simple Open EtherCAT Master), EtherCAT mailbox length validation
Affected	SOEM up to and including v2.0.0
Fixed	SOEM v2.0.1 (2026-10-15)
Type	Out-of-bounds write via integer underflow (CWE-191, CWE-195, CWE-787)
Vendor advisory	RT-Labs RRTL-260921-01
Credit	EunOus (EpsilonOrg), shared with four other independent reporters (CVE record)

Issue

SOEM is an open-source EtherCAT master stack, the software that drives an EtherCAT fieldbus from a PC or an embedded controller. CVE-2026-70388 is an out-of-bounds write reached through an integer underflow in SOEM's validation of mailbox message lengths: a malformed length lets a computed size wrap below zero and drive a write past its intended bound. It sits on the EtherCAT mailbox path, the channel used for the acyclic, higher-level exchanges between the master and a slave device.

Timeline

DATE	EVENT
2026-09-21	RT-Labs advisory RRTL-260921-01
2026-10-15	SOEM v2.0.1 released with the fix
2026-10-26	CVE-2026-70388 record published by ENISA (CNA)

02 Coordinated disclosure

This is a disclosure note, not a full technical write-up. The in-depth analysis of this vulnerability, the exact underflow site, the affected code paths and the fix, was led, coordinated and published by **RT-Labs**, the maintainers of the SOEM ecosystem, in their advisory **RRTL-260921-01**. Epsilon contributed to this disclosure and is credited on the CVE. We link RT-Labs' advisory as the authoritative source rather than restating their work here.

Epsilon's role

Epsilon reported findings in the SOEM EtherCAT stack to RT-Labs during coordinated disclosure. CVE-2026-70388 credits "EunOus / EpsilonOrg" alongside four other independent reporters.

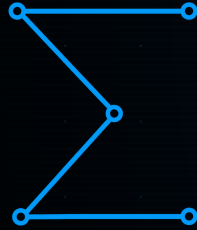
Where to read the technical detail

For the vulnerable function, the precise underflow, the affected versions and the patch, read RT-Labs' advisory and the fixed release directly:

Advisory	rt-labs.com · RRTL-260921-01 (PDF)
Project	github.com/OpenEtherCATsociety/SOEM
Record	CVE-2026-70388 (CVSS 8.3, CNA ENISA, published 2026-10-26)

Mitigation

Update SOEM to v2.0.1 or later, as named in the RT-Labs advisory. Deployments that cannot update immediately should restrict which devices can reach the EtherCAT segment, since the mailbox path is exercised by a device on the bus.



ESPILON

SECURITY RESEARCH

Embedded, IoT and OT security research

espilon.net

eun0us@espilon.net

Association loi 1901 • France