Information tampering and Denial-of-service (DoS) vulnerability in CC-Link IE TSN communication protocol

Release date: July 30, 2026
Mitsubishi Electric Corporation

Overview

An information tampering and denial-of-service (DoS) vulnerability exists in the CC-Link IE TSN communication protocol. An attacker with access to a CC-Link IE TSN network may be able to tamper with communication data by sending specially crafted packets under specific timing conditions (CVE-2026-13584). As a result, the attacker may be able to cause a denial-of-service (DoS) condition in the affected product by interfering with its control function or causing it to operate incorrectly.

CVSS[1]

CVE-2026-13584 CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N Base score 7.1

Affected products

Affected products and versions are shown below.

No.	Product name	Product Model	Version
1	MELSEC MX Controller MX-R model	MXR300-16/32/64 MXR500-128/256	All versions
2	MELSEC MX Controller MX-F model	MXF100-8-N32/P32 MXF100-16-N32/P32	All versions
3	Master/local module	RJ71GN11-T2/SX/EIP	All versions
4		FX5-CCLGN-MS	All versions
5	CC-Link IE TSN interface board	NZ81GN11-SX/T2	All versions
6	Motion module	RD78G4/G8/G16/G64 RD78GHV/GHW	All versions
7		FX5-40SSC-G FX5-80SSC-G	All versions
8	Motion Control Board	MR-EM441G	All versions
9	Block-type remote module	NZ2GN2S1-32D/32T/32TE/32DT/32DTE NZ2GN2B1-32D/32T/32TE/32DT/32DTE NZ2GNCF1-32D/32T NZ2GNCE3-32D/32DT NZ2GN12A4-16D/16DE NZ2GN12A2-16T/16TE NZ2GN12A42-16DT/16DTE NZ2GN2S1-16D/16T/16TE NZ2GN2B1-16D/16T/16TE	All versions
10	Block-type remote module with safety functions	NZ2GNSS2-8D/8TE/16DTE (incl. -K models) NZ2GNS12A2-14DT/16DTE	All versions
11	Analog-Digital converter module	NZ2GN2S-60AD4 NZ2GN2B-60AD4	All versions
12	Digital-Analog converter module	NZ2GN2S-60DA4 NZ2GN2B-60DA4	All versions
13	CC-Link IE TSN compatible coupler[*1]	NZ2FT-GN	All versions
14	FPGA module	NZ2GN2S-D41P01/D41D01/D41PD02	All versions
15	Tension meter	LM7-1LG LM7-2LG	All versions
16	AC Servo MELSERVO-J5	MR-J5-G MR-J5W-G MR-J5-G-HS/RJ/LL MR-J5D-G4 MR-MD333G	All versions
17	AC Servo MELSERVO-JET[*1]	MR-JET-G/G4-HS	All versions
18	Liner Track System MTR-S series Linear track control module[*1]	MTR-SCU00-4G/PG	All versions
19	Inverter FR-A800/F800/E800 Series	FR-A8NCG FR-A8NCG-S FR-A800-GN FR-E800-E/SCE	All versions

[1] https://www.first.org/cvss/v4-0/specification-document

20	Industrial Robot CR800-D series controller Network Base Card	2F-DQ535-TSN	All versions
21	CC-Link IE TSN expansion unit	FCU8-EX569	All versions
22	CC-Link IE TSN-CC-Link IE Field Network bridge module	NZ2GN-GFB	All versions
23	CC-Link IE TSN-AnyWireASLINK bridge module	NZ2AW1GNAL	All versions
24	Energy Measuring Unit CC-Link IE TSN Communication Unit	EMU4-CM-TSN	All versions
25	Industrial Computer MELIPC series	MI2532-W MI2332-W	All versions
26	GOT3000 Series	GT3715-FHCBD GT3712-WXCBD GT3715-XRBA/XRBD GT3712-XRBA/XRBD GT3710-XRBA/XRBD GT3708-XRBA/XRBD	All versions
27	CC-Link IE TSN Communication Unit	GT25-J71GN13-T2	All versions
28	Motion Control Software	SWM-G SWM-G-N1	All versions
29	CC-Link IE TSN Communication Software for Windows	SW1DND-CCIETCT-M	All versions
30	Analysis Support Software MELSOFT VIMA*1	SW1DNN-VIMA-M	All versions
31	Master/Local module Designated communication LSI DeviceKit	NZ2KT-NPETNG51	All versions
32	Master/Local module Designated communication LSI	NZ2GACP610-60	All versions
33	Remote Station Communication LSI with GbE-PHY	NZ2GACP620-60/300 NZ2GACP621-90/720	All versions
34	CC-Link IE TSN Master/Local module Designated communication LSI SDK	SW1DNN-GN610SRC-M	All versions
35	Remote station software development kit	SW1DNC-GNSDK1S-M SW1DNC-GNSDK2S-M	All versions

*1: These products are sold in limited regions.

Description

An information tampering and denial-of-service (DoS) vulnerability exists in the CC-Link IE TSN communication protocol due to Improper Enforcement of Message Integrity During Transmission in a Communication Channel (CWE-924[2]).

Impact

An attacker with access to a CC-Link IE TSN network may be able to tamper with communication data (control input/output values) by sending specially crafted packets under specific timing conditions. As a result, the attacker may be able to cause a denial-of-service (DoS) condition in the affected product by interfering with its control function or causing it to operate incorrectly.

Countermeasures for Customers

Please take the mitigations / workarounds described in the " Mitigations / Workarounds" section.

Mitigations / Workarounds

Mitsubishi Electric recommends that the customers take the following mitigations to minimize the risk of exploitation of this vulnerability.

- To prevent attackers from connecting attack devices, restrict physical access to the affected product and the CC-Link IE TSN network to which the affected products are connected by taking measures such as the following:
  a) Manage access to and from the site where the affected products are installed.
  b) Lock the control panel in which the affected products and/or the network devices are installed.
  c) Lock the Ethernet ports, such as by using port lock accessories.
- Use the affected products within a trusted network where communication with untrusted networks and hosts is blocked by a firewall or similar measures.
- Appropriately configure credentials and access privileges for network devices installed at the boundary between trusted networks and external networks.

Acknowledgement

Mitsubishi Electric would like to thank Alessandro Di Pinto, Giovanni Dini Gentilini, Luca Cremona and Gabriele Quagliarella at Nozomi Networks, Inc. who reported this vulnerability.

2 https://cwe.mitre.org/data/definitions/924.html

Contact information

Please contact your local Mitsubishi Electric representative.

〈Inquiries | MITSUBISHI ELECTRIC FA〉
https://www.mitsubishielectric.com/fa/service-support/index.html