Denial-of-Service Vulnerability in Ethernet function of multiple FA products

Release date: April 25, 2025
Last update date: October 9, 2025
Mitsubishi Electric Corporation

Overview

A denial-of-service (DoS) vulnerability exists in the Ethernet function of multiple FA products. A remote attacker could cause a denial-of-service (DoS) condition in the products by sending specially crafted UDP packets. (CVE-2025-3511)

CVSS[1]

CVE-2025-3511 CVSS:3.1/AV: N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base score 7.5

Affected products

The following products and versions are affected.

No.	Product Name/Series	Model name	Version
1	CC-Link IE TSN Remote I/O 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	versions 09 and prior
2	CC-Link IE TSN Analog-Digital Converter module	NZ2GN2S-60AD4 NZ2GN2B-60AD4	versions 07 and prior
3	CC-Link IE TSN Digital-Analog Converter module	NZ2GN2S-60DA4 NZ2GN2B-60DA4	versions 07 and prior
4	CC-Link IE TSN FPGA module	NZ2GN2S-D41P01/D41D01/D41PD02	version 01
5	CC-Link IE TSN Remote Station Communication LSI CP620 with GbE-PHY	NZ2GACP620-300/60	versions 1.08J and prior
6	MELSEC iQ-R Series CC-Link IE TSN Master/Local Module	RJ71GN11-T2	versions 26 and prior
7		RJ71GN11-EIP	versions 10 and prior
8		RJ71GN11-SX	versions 05 and prior
9	MELSEC iQ-R Series Ethernet Interface Module	RJ71EN71	versions 85 and prior
10	CC-Link IE TSN master/local Station Communication LSI CP610	NZ2GACP610-60 NZ2KT-NPETNG51	versions 05 and prior

【Version check procedure】

No.1-4,10: Please check the firmware version using the "CC-Link IE TSN Firmware Update Tool". For detailed instructions, refer to the help within the "CC-Link IE TSN Firmware Update Tool"

No.5: Install the CP620 sample code and check the version of the CP620 sample code in the "version.txt" file within the created folder. For information on how to get and install the CP620 sample code, refer to the "Update Procedure" in the "Countermeasures for Customers" section.

No.6-9: Refer to "Appendix 1 Checking Production Information and Firmware Version" in the MELSEC iQ-R Module Configuration Manual to check the firmware version of the product. The manual can be downloaded from the following site.
https://www.mitsubishielectric.com/fa/download/index.html

Description

A denial-of-service (DoS) vulnerability due to Improper Validation of Specified Quantity in Input (CWE-1284[2]) exists in the Ethernet function of multiple FA products.

Impact

A remote attacker could cause a denial-of-service (DoS) condition in the products by sending specially crafted UDP packets.

No.1-5: The threat arises when the affected product does not receive a valid UDP packet within 3 seconds after receiving a specially crafted UDP packet from a remote attacker. A system reset of the product is required for recovery.

No.6-10: The threat arises when the affected product receives a specially crafted UDP packet from a remote attacker. A system reset of the product is required for recovery.

[1] https://www.first.org/cvss/v3-1/specification-document

[2] https://cwe.mitre.org/data/definitions/1284.html

Countermeasures for Customers

Customers using the affected products should follow the steps below to update the firmware or the CP620 sample code to the fixed version described in the “Countermeasures for Products” section.

【Update Procedure】

Please download the fixed update file or the CP620 sample code described in the “Countermeasures for Products” section, the engineering software and the manual for the firmware version updates from the website below and update to fixed version.

https://www.mitsubishielectric.com/fa/download/index.html

For the update procedure, please refer to the following.

No.1-4,10:

・CC-Link IE TSN Firmware Update Tool Reference Manual “2. FIRMWARE UPDATE PROCEDURE”

No.5:

・CP620 sample code could be installed by running 'SW1DNC-GN620SRC-M.exe' within the downloaded file.

No.6-9:

・"Appendix 2 Firmware Update Function" in the MELSEC iQ-R Module Configuration Manual

Countermeasures for Products

The series, product names, and versions in which the vulnerability has been fixed are as follows.

No.	Product Name/Series	Model name	Version
1	CC-Link IE TSN Remote I/O 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	version 10 or later
2	CC-Link IE TSN Analog-Digital Converter module	NZ2GN2S-60AD4 NZ2GN2B-60AD4	version 08 or later
3	CC-Link IE TSN Digital-Analog Converter module	NZ2GN2S-60DA4 NZ2GN2B-60DA4	version 08 or later
4	CC-Link IE TSN FPGA module	NZ2GN2S-D41P01/D41D01/D41PD02	version 02 or later
5	CC-Link IE TSN Remote Station Communication LSI CP620 with GbE-PHY	NZ2GACP620-300/60	version 1.09K or later
6	MELSEC iQ-R Series CC-Link IE TSN Master/Local Module	RJ71GN11-T2	version 28 or later
7		RJ71GN11-EIP	version 13 or later
8		RJ71GN11-SX	version 07 or later
9	MELSEC iQ-R Series Ethernet Interface Module	RJ71EN71	version 86 or later
10	CC-Link IE TSN master/local Station Communication LSI CP610	NZ2GACP610-60 NZ2KT-NPETNG51	version 06 or later

Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:

- Use a firewall, virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Restrict physical access to the affected products and the LAN to which they are connected.
- Install anti-virus software on your PC that can access the product.

Contact information

Please contact your local Mitsubishi Electric representative.

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

Update history

October 9, 2025

Affected products, Impact, Countermeasures for Customers, Countermeasures for Products have been revised.

The affected products RJ71GN11-T2, RJ71GN11-EIP, RJ71GN11-SX, RJ71EN71, NZ2GACP610-60 and NZ2KT-NPETNG51 have been added.