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

Release date: February 27, 2024
Last update date: January 16, 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 temporary denial-of-service (DoS) condition for a certain period of time in the Ethernet communication of the products by performing TCP SYN Flood attack*1. (CVE-2023-7033)

*1: A type of DoS attack in which an attacker sends a large number of SYN packets requesting TCP connections.

CVSS[1]

CVE-2023-7033 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score 5.3

Affected products

The following products and versions are affected:

Series	Product name	Version
MELSEC iQ-R series CPU module	R00/01/02CPU	All versions
	R04/08/16/32/120(EN)CPU	All versions
	R08/16/32/120SFCPU	All versions
	R08/16/32/120PCPU	All versions
	R08/16/32/120PSFCPU	All versions
MELSEC iQ-L series CPU module	L04/08/16/32HCPU*2	All versions
MELSEC iQ-R Ethernet Interface Module	RJ71EN71	All versions
MELSEC iQ-R CC-Link IE TSN Master/Local Module	RJ71GN11-T2, RJ71GN11-SX, RJ71GN11-EIP	All versions
CC-Link IE TSN Remote I/O Module	NZ2GN2B1-32D/32T/32TE/32DT/32DTE	All versions
	NZ2GN2B1-16D/16T/16TE	All versions
	NZ2GN2S1-32D/32T/32TE/32DT/32DTE	All versions
	NZ2GN2S1-16D/16T/16TE	All versions
	NZ2GNCF1-32D/32T	All versions
	NZ2GNCE3-32D/32DT	All versions
	NZ2GN12A4-16D/16DE	All versions
	NZ2GN12A2-16T/16TE	All versions
	NZ2GN12A42-16DT/16DTE	All versions
CC-Link IE TSN Analog-Digital Converter Module	NZ2GN2S/NZ2GN2B-60AD4	All versions
CC-Link IE TSN Digital-Analog Converter Module	NZ2GN2S/NZ2GN2B-60DA4	All versions
CC-Link IE TSN - CC-Link IE Field Network Bridge Module	NZ2GN-GFB	All versions
CC-Link IE TSN - AnyWireASLINK Bridge Module	NZ2AW1GNAL	All versions
CC-Link IE TSN FPGA Module	NZ2GN2S-D41P01/D41D01/D41PD02	All versions
CC-Link IE TSN Remote Station Communication LSI CP620 with GbE-PHY	NZ2GACP620-300/60	All versions

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

Series	Product name	Version
MELSEC iQ-R Motion Module	RD78G4/8/16/32/64/HV/HW	All versions
MELSEC iQ-L Motion Module	LD78G4/16*2	All versions
MELSEC iQ-F FX5 Motion Module	FX5-xSSC-G (x=40,80)	All versions
MELSEC iQ-F Series CPU module	FX5U-xMy/z (x=32,64,80, y=T,R, z=ES,DS,ESS,DSS)	All versions
	FX5UC-xMy/z (x=32,64,96, y=T, z=D,DSS)	All versions
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	All versions
	FX5UJ-xMy/z (x=24,40,60, y=T,R, z=ES,DS,ESS,DSS)	All versions
	FX5UJ-xMy/ES-A*2 (x=24,40,60, y=T,R)	All versions
	FX5S-xMy/z (x=30,40,60,80*2, y=T,R, z=ES,ESS)	All versions
MELSEC iQ-F Series Ethernet module	FX5-ENET	All versions
MELSEC iQ-F Series Ethernet/IP module	FX5-ENET/IP	All versions
MELSEC iQ-F Series OPC UA Module	FX5-OPC	All versions
MELSEC iQ-F Series CC-Link IE TSN master/local module	FX5-CCLGN-MS	All versions
GOT2000 Series CC-Link IE TSN Communication Unit	GT25-J71GN13-T2	All versions
FR-A800-E series inverters	FR-A800-E series	All versions
FR-F800-E series inverters	FR-F800-E series	All versions
FR-E800-E series inverters	FR-E800-E series	All versions
INVERTER CC-Link IE TSN Plug-in option	FR-A8NCG	All versions
INVERTER CC-Link IE TSN Safety Plug-in option	FR-A8NCG-S	All versions
INVERTER CC-Link IE TSN communication function built-in type	FR-A800-GN	All versions
MR-J5 series AC Servos MELSERVO	MR-J5-A series, MR-J5-G series, MR-J5W-G series, MR-J5D-G series	All versions
MR-JET series AC Servos MELSERVO	MR-JET-G series*2	All versions
MR-MD333G series AC Servos MELSERVO	MR-MD333G series	All versions
MR-JE series AC Servos MELSERVO	MR-JE-C series*2	All versions
MELSERVO-J4 AC Servos MELSERVO	MR-J4-GF series	version A4 or later
Embedded Type Servo System Controller	MR-EM441G series	All versions

*2: These products are sold in limited regions.

Description

A denial-of-service (DoS) vulnerability due to Insufficient Resource Pool (CWE-410[2]) exists in the Ethernet function of multiple FA products.

Impact

A remote attacker could cause a temporary denial-of-service (DoS) condition for a certain period of time in the Ethernet communication of the products by performing TCP SYN Flood attack.

Countermeasures for Customers

There are no plans to release a fixed version, so we kindly ask you to address this issue through mitigations and workarounds.

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.
- Use IP filter function*3 to block access from untrusted hosts.
- Restrict physical access to the affected products and the LAN to which they are connected.

*3: The IP filter function can be set on the following models. For details on the IP filter function, please refer to the following manual for each product.
"1.13 IP Filter" in the MELSEC iQ-R Ethernet User's Manual (Application)
MELSEC iQ-L CPU 模块用户手册(应用篇) 24.1 IP 滤波器功能
"1.4 Security/IP filter" in the MELSEC iQ-R Motion Module User's Manual (Network)

[2] https://cwe.mitre.org/data/definitions/410.html

"3.5 Security/IP filter" in the MELSEC iQ-F FX5 Motion Module User's Manual (CC-Link IE TSN)
"13.1 IP Filter Function" in the MELSEC iQ-F FX5 User's Manual (Communication)
"12.1 IP Filter Function" in the MELSEC iQ-F FX5 User's Manual (Ethernet Communication)
"4.4 IP Filter" in the MELSEC iQ-F FX5 OPC UA Module User's Manual
"4.5.1 IP Filter" in the MELSEC iQ-F FX5 OPC UA Module User's Manual

Contact information

Please contact your local Mitsubishi Electric representative.

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

Update history

January 16, 2025
Added Affected products.
R00/01/02CPU, R04/08/16/32/120(EN)CPU, R08/16/32/120SFCPU, R08/16/32/120PCPU, R08/16/32/120PSFCPU, L04/08/16/32HCPU,
RJ71EN71, RJ71GN11-T2, RJ71GN11-SX, RJ71GN11-EIP, NZ2GN2B1-32D/32T/32TE/32DT/32DTE, NZ2GN2B1-16D/16T/16TE, NZ2GN2S1-32D/32T/32TE/32DT/32DTE, NZ2GN2S1-16D/16T/16TE, NZ2GNCF1-32D/32T, NZ2GNCE3-32D/32DT, NZ2GN12A4-16D/16DE, NZ2GN12A2-16T/16TE, NZ2GN12A42-16DT/16DTE, NZ2GN2S/NZ2GN2B-60AD4, NZ2GN2S/NZ2GN2B-60DA4, NZ2GN-GFB, NZ2AW1GNAL, NZ2GN2S-D41P01/D41D01/D41PD02, NZ2GACP620-300/60, RD78G4/8/16/32/64/HV/HW, LD78G4/16, FX5-xSSC-G, FX5-ENET, FX5-ENET/IP, FX5-OPC, FX5-CCLGN-MS, GT25-J71GN13-T2, FR-A800-E series, FR-F800-E series, FR-E800-E series, FR-A8NCG, FR-A8NCG-S, FR-A800-GN, MR-J5-A series, MR-J5-G series, MR-J5W-G series, MR-J5D-G series, MR-JET-G series, MR-MD333G series, MR-JE-C series, MR-J4-GF series, MR-EM441G series

Changed "Countermeasures" to "Countermeasures for Customers".