America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Mitsubishi Electric Multiple FA Products (Update B)

Last Revised: February 03, 2026 **Alert Code:** ICSA-25-128-03

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf/blob/develop/csaf_files/ot/white/2025/icsa-25-128-03.json>

Summary

Successful exploitation of this vulnerability could allow an remote attacker to cause a denial-of-service condition on the affected products.

The following versions of Mitsubishi Electric FA Products are affected:

- CC-Link IE TSN Remote I/O module NZ2GN2S1-32D <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2S1-32T <=09 (CVE-2025-3511)

- CC-Link IE TSN Remote I/O module NZ2GN2S1-32TE <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2S1-32DT <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2S1-32DTE <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2B1-32D <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2B1-32T <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2B1-32TE <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2B1-32DT <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2B1-32DTE <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GNCF1-32D <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GNCF1-32T <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GNCE3-32D <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GNCE3-32DT <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN12A4-16D <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN12A4-16DE <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN12A2-16T <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN12A2-16TE <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN12A42-16DT <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN12A42-16DTE <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2S1-16D <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2S1-16T <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2S1-16TE <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2B1-16D <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2B1-16T <=09 (CVE-2025-3511)
- CC-Link IE TSN Remote I/O module NZ2GN2B1-16TE <=09 (CVE-2025-3511)
- CC-Link IE TSN Analog-Digital Converter module NZ2GN2S-60AD4 <=07 (CVE-2025-3511)
- CC-Link IE TSN Analog-Digital Converter module NZ2GN2B-60AD4 <=07 (CVE-2025-3511)
- CC-Link IE TSN Digital-Analog Converter module NZ2GN2S-60DA4 <=07 (CVE-2025-3511)

- CC-Link IE TSN Digital-Analog Converter module NZ2GN2B-60DA4 <=07 (CVE-2025-3511)
- CC-Link IE TSN FPGA module NZ2GN2S-D41P01 01 (CVE-2025-3511)
- CC-Link IE TSN FPGA module NZ2GN2S- D41D01 01 (CVE-2025-3511)
- CC-Link IE TSN FPGA module NZ2GN2S-D41PD02 01 (CVE-2025-3511)
- CC-Link IE TSN Remote Station Communication LSI CP620 with GbE-PHY NZ2GACP620-300 <=1.08J (CVE-2025-3511)
- CC-Link IE TSN Remote Station Communication LSI CP620 with GbE-PHY NZ2GACP620-60 <=1.08J (CVE-2025-3511)
- MELSEC iQ-R Series CC-Link IE TSN Master/Local Module RJ71GN11-T2 <=26 (CVE-2025-3511)
- MELSEC iQ-R Series CC-Link IE TSN Master/Local Module RJ71GN11-EIP <=10 (CVE-2025-3511)
- MELSEC iQ-R Series CC-Link IE TSN Master/Local Module RJ71GN11-SX <=05 (CVE-2025-3511)
- MELSEC iQ-R Series Ethernet Interface Module RJ71EN71 <=85 (CVE-2025-3511)
- CC-Link IE TSN master/local Station Communication LSI CP610 NZ2GACP610-60 <=05 (CVE-2025-3511)
- CC-Link IE TSN master/local Station Communication LSI CP610 NZ2KT-NPETNG51 <=05 (CVE-2025-3511)
- MELSEC iQ-F Series FX5 CC-Link IE TSN Master/Local Module FX5-CCLGN-MS vers:all/* (CVE-2025-3511)
- MELSEC iQ-F Series FX5 Ethernet Module FX5-ENET <=1.200 (CVE-2025-3511)
- MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP vers:all/* (CVE-2025-3511)

CVSS	Vendor	Equipment	Vulnerabilities
v3 7.5	Mitsubishi Electric	Mitsubishi Electric FA Products	Improper Validation of Specified Quantity in Input

Background

- **Critical Infrastructure Sectors:** Critical Manufacturing
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** Japan

Vulnerabilities

Expand All +

CVE-2025-3511 +

Acknowledgments

- Mitsubishi Electric reported this vulnerability to CISA

Legal Notice and Terms of Use

This product is provided subject to this Notification (https://www.cisa.gov/notification) and this Privacy & Use policy (https://www.cisa.gov/privacy-policy).

Recommended Practices

CISA recommends users take defensive measures to minimize the exploitation risk of these vulnerabilities.

Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolate them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most recent version available. Also recognize VPN is only as secure as its connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

Advisory Conversion Disclaimer

This ICSA is a verbatim republication of CISA ICSA-25-128-03 from a direct conversion of the vendor's Common Security Advisory Framework (CSAF) advisory. This is republished to CISA's website as a means of increasing visibility and is provided "as-is" for informational purposes only. CISA is not responsible for the editorial or technical accuracy of republished advisories and provides no warranties of any kind regarding any information contained within this advisory. Further, CISA does not endorse any commercial product or service. Please contact CISA directly for any questions regarding this advisory.

Revision History

- **Initial Release Date:** 2025-05-08

Date	Revision	Summary
2025-05-08	1	Initial Publication
2025-10-09	2	Update A - Update to 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.

Date	Revision	Summary
2026-02-03	3	Update B - Update to Summary, Affected products, and Remediations have been revised. The affected products FX5-CCLGN-MS, FX5-ENET, and FX5-ENET/IP have been added.
2026-02-03	4	CISA Republication update based on CISA ICSA-25-128-03 advisory

Legal Notice and Terms of Use

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Mitsubishi Electric

Tags

Sector: Critical Manufacturing Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-04

SpiceJet Online Booking System </news-events/ics-advisories/icsa-26-113-04>

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-06

Intrado 911 Emergency Gateway (EGW) </news-events/ics-advisories/icsa-26-113-06>

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-02

Carlson Software VASCO-B GNSS Receiver </news-events/ics-advisories/icsa-26-113-02>

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-01

Yadea T5 Electric Bicycle </news-events/ics-advisories/icsa-26-113-01>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov