



## America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

### ICS ADVISORY

# Mitsubishi Electric Multiple FA Products (Update C)

**Last Revised:** April 30, 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](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 a remote attacker to cause a denial-of-service (DoS) condition, a timeout error, or a communication delay by sending a specially crafted UDP packet to the product.**

The following versions of Mitsubishi Electric Multiple FA Products are affected:

- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2S1-32D <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2S1-32T <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2S1-32TE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2S1-32DT <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2S1-32DTE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2B1-32D <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2B1-32T <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2B1-32TE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2B1-32DT <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2B1-32DTE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCF1-32D <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCF1-32T <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCF1-32TE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCF1-32DT <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCF1-32DTE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCE3-32D <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCE3-32T <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCE3-32TE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCE3-32DT <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GNCE3-32DTE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN12A4-16D <=09 (CVE-2025-3511)

- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN12A4-16DE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN12A2-16T <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN12A2-16TE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN12A42-16DT <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN12A42-16DTE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2S1-16D <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2S1-16T <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2S1-16TE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2B1-16D <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2B1-16T <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote I/O module NZ2GN2B1-16TE <=09 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Analog-Digital Converter module NZ2GN2S-60AD4 <=07 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Analog-Digital Converter module NZ2GN2B-60AD4 <=07 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Digital-Analog Converter module NZ2GN2S-60DA4 <=07 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Digital-Analog Converter module NZ2GN2B-60DA4 <=07 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN FPGA module NZ2GN2S-D41P01 01 (CVE-2025-3511)

- Mitsubishi Electric CC-Link IE TSN FPGA module NZ2GN2S-D41D01 01 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN FPGA module NZ2GN2S-D41PD02 01 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote Station Communication LSI CP620 with GbE-PHY NZ2GACP620-300 <=1.08J (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN Remote Station Communication LSI CP620 with GbE-PHY NZ2GACP620-60 <=1.08J (CVE-2025-3511)
- Mitsubishi Electric MELSEC iQ-R Series CC-Link IE TSN Master/Local Module RJ71GN11-T2 <=26 (CVE-2025-3511)
- Mitsubishi Electric MELSEC iQ-R Series CC-Link IE TSN Master/Local Module RJ71GN11-EIP <=10 (CVE-2025-3511)
- Mitsubishi Electric MELSEC iQ-R Series CC-Link IE TSN Master/Local Module RJ71GN11-SX <=05 (CVE-2025-3511)
- Mitsubishi Electric MELSEC iQ-R Series Ethernet Interface Module RJ71EN71 <=85 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN master/local Station Communication LSI CP610 NZ2GACP610-60 <=05 (CVE-2025-3511)
- Mitsubishi Electric CC-Link IE TSN master/local Station Communication LSI CP610 NZ2KT-NPETNG51 <=05 (CVE-2025-3511)
- Mitsubishi Electric MELSEC iQ-F Series FX5 CC-Link IE TSN Master/Local Module FX5-CCLGN-MS <=1.020 (CVE-2025-3511)
- Mitsubishi Electric MELSEC iQ-F Series FX5 Ethernet Module FX5-ENET <=1.200 (CVE-2025-3511)
- Mitsubishi Electric MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP <=1.106 (CVE-2025-3511)

| CVSS   | Vendor              | Equipment                                | Vulnerabilities                                    |
|--------|---------------------|--|--|
| v3 7.5 | Mitsubishi Electric | Mitsubishi Electric Multiple 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](https://www.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](https://www.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 Mitsubishi Electric 2025-001 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 Mitsubishi Electric directly for any questions regarding this advisory.

## Revision History

- **Initial Release Date:** 2025-04-25

| Date       | Revision | Summary   |
|------------|----------|---|
| 2025-04-25 | 1        | Initial Republication   |
| 2025-10-09 | 2        | CISA Republication - 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        | CISA Republication - 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.                                       |
| 2026-04-30 | 4        | CISA Republication - Update C - Added FX5-CCLGN-MS and FX5-ENET/IP that have been fixed to Countermeasures for Products. Affected products, Countermeasures for Customers, and Countermeasures for Products have been revised. |

---

## Legal Notice and Terms of Use

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) 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 30, 2026 ■ ICS ADVISORY | ICSA-26-120-04

APR 30, 2026 ■ ICS ADVISORY | ICSA-26-120-06

## [ABB Ability OPTIMAX](#)

[events/ics-advisories/icsa-26-120-04](#)

APR 30, 2026 ■ ICS ADVISORY | ICSA-26-120-03

## [ABB Edgenius Management](#)

[Portal](#)  
[03](#)

## [ABB Ability Symphony Plus](#)

[Engineering](#)  
[advisories/icsa-26-120-06](#)

APR 30, 2026 ■ ICS ADVISORY | ICSA-26-120-02

## [ABB PCM600](#)

[advisories/icsa-26-120-02](#)

[Return to top](#)

[Topics](#)

[Spotlight](#)

[Resources & Tools](#)

[News & Events](#)

[Careers](#)

[About](#)



**CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**



**CISA Central**

1-844-Say-CISA

[contact@cisa.dhs.gov](mailto:contact@cisa.dhs.gov)



[CISA.gov](https://www.cisa.gov)

An official website of the U.S. Department of Homeland Security

[About CISA](#)

[Budget and Performance](#)

[DHS.gov](https://www.dhs.gov)

<https://www.dhs.gov/performance-financial-reports>

[FOIA Requests](https://www.dhs.gov/foia)  
<<https://www.dhs.gov/foia>>

[No FEAR Act](#) </no-fear-act>

[Office of Inspector General](https://www.oig.dhs.gov/)  
<<https://www.oig.dhs.gov/>>

[Privacy Policy](#) </privacy-policy>

[Subscribe](#)

[The White House](https://www.whitehouse.gov/)  
<<https://www.whitehouse.gov/>>

[USA.gov](https://www.usa.gov/) <<https://www.usa.gov/>>

[Website Feedback](/forms/feedback) </forms/feedback>