



# Denial-of-Service (DoS) vulnerability in Ethernet function of MELSEC iQ-F Series EtherNet/IP module and Ethernet module

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-1874
<b>State</b>	PUBLISHED
<b>Assigner</b>	Mitsubishi
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-03 07:16:10 UTC
<b>Updated</b>	2026-04-24 08:16:29 UTC
<b>Description</b>	Always-Incorrect Control Flow Implementation vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5-EN

## Risk And Classification

**Primary CVSS:** v4.0 8.7 HIGH from Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-670 | CWE-670 CWE-670 Always-Incorrect Control Flow Implementation

Version	Source	Type	Score	Severity	Vector
4.0	Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Mitsubishi Electric Corporation</a>	<a href="#">MELSEC IQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP</a>	affected versions 1.106 and
CNA	<a href="#">Mitsubishi Electric Corporation</a>	<a href="#">MELSEC IQ-F Series FX5-EIP EtherNet/IP Module FX5-EIP</a>	affected versions 1.000 and

### References

Reference	Source	Link
<a href="http://www.cisa.gov/news-events/ics-advisories/icsa-26-62-01">www.cisa.gov/news-events/ics-advisories/icsa-26-62-01</a>	<a href="mailto:Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp">Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp</a>	<a href="http://www.cisa.gov">www.cisa.gov</a>
<a href="http://jvn.jp/vu/JVNVU93286687">jvn.jp/vu/JVNVU93286687</a>	<a href="mailto:Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp">Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp</a>	<a href="http://jvn.jp">jvn.jp</a>
<a href="http://www.mitsubishielectric.com/psirt/vulnerability/pdf/2025-021_en.pdf">www.mitsubishielectric.com/psirt/vulnerability/pdf/2025-021_en.pdf</a>	<a href="mailto:Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp">Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp</a>	<a href="http://www.mitsubishielec">www.mitsubishielec</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)