Denial-of-Service(DoS) Vulnerability in TCP Communication Function on MELSEC iQ-F Series CPU module

Release date: November 6, 2025
Mitsubishi Electric Corporation

Overview

Denial-of-Service (DoS) vulnerability exists in the TCP communication function on the MELSEC iQ-F Series CPU module. A remote attacker may be able to disconnect the connection by sending specially crafted TCP packets to cause a denial-of-service (DoS) condition on the products (CVE-2025-10259). There is no impact on connections other than the attacked one.

CVSS[1]

CVE-2025-10259 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 are affected:

Series	Product name	Version
MELSEC iQ-F Series	FX5U-xMT/y, FX5U-xMR/z x=32,64,80, y=ES,DS,ESS,DSS, z=ES,DS	All versions
	FX5UC-xMT/y x=32,64,96, y=D,DSS	All versions
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	All versions
	FX5UJ-xMT/y, FX5UJ-xMR/z x=24,40,60, y=ES,DS,ESS,DSS, z=ES,DS	All versions
	FX5UJ-xMy/ES-A*1 x=24,40,60, y=T,R	All versions
	FX5S-xMT/y, FX5S-xMR/z x=30,40,60,80*1, y=ES,DS,ESS,DSS, z=ES,DS	All versions
	FX5S-xMy/ES-A*1 x=30,40,60,80, y=T,R	All versions

*1: These products are sold in limited regions.

Description

Denial-of-Service (DoS) vulnerability due to Improper Validation of Specified Quantity in Input(CWE-1284[2]) exists in the TCP communication function on the MELSEC iQ-F Series CPU module.

Impact

A remote attacker may be able to disconnect the connection by sending specially crafted TCP packets to cause a denial-of-service (DoS) condition on the products. There is no impact on connections other than the attacked one. Also, in order to recovery, it is necessary to re-establish the connection.

Countermeasures for Customers

There are no plans to release a fixed version, so please take the following mitigations / workarounds.

Mitigations / Workarounds

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

- Use a virtual private network (VPN) to encrypt the communication when Internet access is required.
- Restrict physical access to the affected products and the LAN that is connected by them.

Acknowledgement

Mitsubishi Electric would like to thank Qian Zou, Ke Xu, Xuewei Feng, Qi Li, Xueying Li, and Gang Jin from Zhongguancun Laboratory at Tsinghua University who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.

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

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

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