# Denial-of-Service(DoS) Vulnerability in Web server function on MELSEC iQ-F Series CPU module

Release date: August 21, 2025
Mitsubishi Electric Corporation

## Overview

Denial-of-Service (DoS) vulnerability exists in the Web server function of the MELSEC iQ-F Series CPU module. A remote attacker may be able to delay the processing of the Web server function and prevent legitimate users from utilizing the Web server function, by sending a specially crafted HTTP request. (CVE-2025-5514)

## CVSS[1]

CVE-2025-5514 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-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS | 1.060 and later |
| | FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS | 1.060 and later |
| | FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS | 1.060 and later |
| | FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,DS,ESS,DSS | All versions |
| | FX5UJ-xMy/ES-A*[1] x=24,40,60, y=T,R, | All versions |
| | FX5S-xMy/z x=30,40,60,80*[1], y=T,R, z= ES,DS,ESS,DSS | All versions |

*1: These products are sold in limited regions.

Please refer to the following manual for how to check the version.
- "17.3 Troubleshooting Using the Engineering Tool" – "Module diagnostics" in the MELSEC iQ-F FX5S/FX5UJ/FX5U/FX5UC User's Manual (Hardware)

Please download the manual from the following URL.
https://www.mitsubishielectric.com/fa/download/index.html

## Description

Denial-of-Service(DoS) vulnerability due to Improper Handling of Length Parameter Inconsistency(CWE-130[2]) exists in the Web server function of the MELSEC iQ-F Series CPU module.

## Impact

A remote attacker may be able to delay the processing of the Web server function and prevent legitimate users from utilizing the Web server function, by sending a specially crafted HTTP request.

## 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 firewall or 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*2 to block access from untrusted hosts.
- Restrict physical access to the affected products and the LAN that is connected by them.

*2: For details on the IP filter function, please refer to the following manual for each product.
"13.1 IP Filter Function" in the MELSEC iQ-F FX5 User's Manual (Communication)

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

2 https://cwe.mitre.org/data/definitions/130.html

## Acknowledgement

Mitsubishi Electric would like to thank Thai Do, Minh Pham, Quan Le, and Loc Nguyen from OPSWAT Unit515 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