# Denial-of-Service Vulnerability in MELSEC iQ-F Series

Release date: July 3, 2025
Mitsubishi Electric Corporation

## Overview

Denial-of-Service (DoS) vulnerability exists in MELSEC iQ-F series due to Overly Restrictive Account Lockout Mechanism(CWE-645[1]). A remote attacker could lockout a legitimate user for a certain period of time by repeatedly attempting to login with an incorrect password.(CVE-2025-5241)

The product models and firmware versions affected by this vulnerability are listed below.

## CVSS[2]

CVE-2025-5241 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

Affected products and firmware versions are below.

| Series | Product name | Version |
|---|---|---|
| MELSEC iQ-F Series | FX5U-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS | All Versions |
| | FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS | All Versions |
| | FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS | All Versions |
| | 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 |
| | FX5-CCLGN-MS | All Versions |

*1 : These products are sold in limited regions

## Description

Denial-of-Service (DoS) vulnerability exists in MELSEC iQ-F series due to Overly Restrictive Account Lockout Mechanism (CWE-645).

## Impact

If the product repeatedly receives login requests with incorrect passwords, it locks out communication to the port on which the requests were received for a certain period of time. An attacker could lockout legitimate users for a certain period by repeatedly attempting to login with incorrect passwords. When the product repeatedly receives unauthorized logins from attacker, legitimate users will be unable to login until a certain period has passed after the lockout or until the product is reset.

## 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)
"4.5 Security" in the MELSEC iQ-F FX5 CC-Link IE TSN Master/Local Module User's Manual

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

## Acknowledgement

Mitsubishi Electric would like to thank Thai Do, Minh Pham, Quan Le and Loc Nguyen of Unit 515, OPSWAT.

[1] https://cwe.mitre.org/data/definitions/645.html

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

## Contact information

Please contact your local Mitsubishi Electric representative.

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