Denial-of-Service Vulnerability in Ethernet function of multiple FA products

Release date: February 27, 2024
Mitsubishi Electric Corporation

Overview

A denial-of-service (DoS) vulnerability exists in the Ethernet function of multiple FA products. A remote attacker could cause a temporary denial-of-service (DoS) condition for a certain period of time in the Ethernet communication of the products by performing TCP SYN Flood attack*1. (CVE-2023-7033)

*1: A type of DoS attack in which an attacker sends a large number of SYN packets requesting TCP connections.

CVSS[1]

CVE-2023-7033 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 and versions 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	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*2 x=24,40,60, y=T,R	All versions
	FX5S-xMy/z x=30,40,60,80*2, y=T,R, z=ES,ESS	All versions

*2: These products are sold in limited regions.

Description

A denial-of-service (DoS) vulnerability due to Insufficient Resource Pool (CWE-410[2]) exists in the Ethernet function of multiple FA products.

Impact

A remote attacker could cause a temporary denial-of-service (DoS) condition for a certain period of time in the Ethernet communication of the products by performing TCP SYN Flood attack.

Countermeasures

Please carry out 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, 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*3 to block access from untrusted hosts.
- Restrict physical access to the affected products and the LAN to which they are connected.

*3: 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)

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/410.html