Denial-of-Service（DoS） Vulnerability in MELSEC Series

Release date: November 2, 2023
Mitsubishi Electric Corporation

Overview

A denial-of-service (DoS) vulnerability exists in the MELSEC-F Series main modules and MELSEC iQ-F Series CPU modules. A remote attacker may be able to reset the memory of the products to factory default state and cause denial-of-service (DoS) condition on the products by sending specific packets. (CVE-2023-4699)

CVSS[1]

CVE-2023-4699 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H Base Score 9.1

Affected products

The following products are affected:

Series	Product name	Version
MELSEC-F series	FX3U-xMy/z x=16,32,48,64,80,128, y=T,R, z=ES,ESS,DS,DSS *1	All versions
	FX3U-32MR/UA1, FX3U-64MR/UA1 *1	
	FX3U-32MS/ES, FX3U-64MS/ES *1	
	FX3U-xMy/ES-A x=16,32,48,64,80,128, y=T,R *1*2	
	FX3UC-xMT/z x=16,32,64,96, z=D,DSS *1	
	FX3UC-16MR/D-T, FX3UC-16MR/DS-T *1	
	FX3UC-32MT-LT, FX3UC-32MT-LT-2 *1	
	FX3UC-16MT/D-P4, FX3UC-16MT/DSS-P4 *1*2	
	FX3G-xMy/z x=14,24,40,60, y=T,R, z=ES,ESS,DS,DSS *1	
	FX3G-xMy/ES-A x=14,24,40,60, y=T,R *1*2	
	FX3GC-32MT/D, FX3GC-32MT/DSS *1	
	FX3GE-xMy/z x=24,40, y=T,R, z=ES,ESS,DS,DSS *2	
	FX3GA-xMy-CM x=24,40,60, y=T,R *1*2	
	FX3S-xMy/z x=10,14,20,30, y=T,R, z=ES,ESS,DS,DSS *1	
	FX3S-30My/z-2AD y=T,R, z=ES,ESS *1	
	FX3SA-xMy-CM x=10,14,20,30, y=T,R *1*2	
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	
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,ESS,DS,DSS	
	FX5UJ-xMy/ES-A x=24,40,60, y=T,R *2	
	FX5S-xMy/z x=30,40,60,80*2, y=T,R, z=ES,ESS	

*1 : These products are affected by the vulnerability if they are used with Ethernet Communication Special Adapter FX3U-ENET-ADP or Ethernet Communication block FX3U-ENET(-L).

*2 : These products are sold in limited regions.

Description

A denial-of-service (DoS) vulnerability due to Insufficient Verification of Data Authenticity (CWE-345[2]) exists in the MELSEC-F Series main modules and MELSEC iQ-F Series CPU modules.

Impact

A remote attacker may be able to reset the memory of the products to factory default state and cause denial-of-service (DoS) condition on the products by sending specific packets.

Countermeasures

Please carry out mitigations/workarounds.

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

[2] https://cwe.mitre.org/data/definitions/345.html

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.
- For MELSEC iQ-F Series, use IP filter function* to block access from untrusted hosts.
- Restrict physical access to the affected products and the LAN that is connected by them.

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

Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>

https://www.mitsubishielectric.com/fa/support/index.html