Authentication Bypass Vulnerability in MELSEC-F Series main module

Release date: June 29, 2023
Mitsubishi Electric Corporation

■Overview

An authentication bypass vulnerability exists in the MELSEC-F Series main modules. A remote attacker may be able to login to the product by sending specially crafted packets. (CVE-2023-2846)

■CVSS[1]

CVE-2023-2846 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score 7.5

■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 version
	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-16MR/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	

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

■Description

An authentication bypass vulnerability due to Authentication Bypass by Capture-replay (CWE-294[2]) exists in the MELSEC-F series main modules.

■Impact

A remote attacker may be able to cancel the password/keyword setting and login to the product by sending specially crafted packets.

■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 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.
- Restrict physical access to affected products and the LAN that is connected by them.

■Acknowledgement

Mitsubishi Electric would like to thank Chun Liu, Xin Che, Ruilong Deng, Peng Cheng, and Jiming Chen from 307LAB, Zhejiang University who reported this vulnerability.

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/294.html

■Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>

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