Arbitrary Command Execution Vulnerability in Mitsubishi Electric proprietary protocol communication of multiple FA products

Release date: November 2, 2023
Last update date: November 12
Mitsubishi Electric Corporation

Overview

Arbitrary command execution vulnerability exists in Mitsubishi Electric proprietary protocol communication used in multiple FA products. A remote attacker may be able to execute arbitrary commands by sending specific packets to the affected products. This could lead to disclose or tamper with information by reading or writing control programs, or cause a denial-of-service (DoS) condition on the products by resetting the memory contents of the products to factory settings or resetting the products remotely. (CVE-2023-4699)

CVSS[1]

CVE-2023-4699 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H Base Score 10.0

Affected products

The following products are affected:

Series	Product name	Version
MELSEC-F series CPU module	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	
	FX5-xSSC-G x=40,80	
	FX5-xSSC-S x=40,80	
MELSEC iQ-R series CPU module	R04/08/16/32/120(EN)CPU	All versions
	R08/16/32/120PCPU	
	R16/32/64MTCPU	
MELSEC iQ-R series	RD78G4/8/16/32/64/HV/HW	All versions
	RD77MS2/4/8/16	
	RD77GF4/8/16/32	
MELSEC iQ-L series	LD78G4/16 *2	All versions
MELSEC Q series	Q172/173DSCPU	All versions
	Q170MSCPU	
	QD77MS2/4/16	
	QD77GF4/8/16	
MELSEC L	LD77MS2/4/16	

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

*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.

Series	Product name	System Number (**indicates the version)	Version
Mitsubishi Electric CNC M800V/M80V series	M800VW	BND-2051W000-**	All versions
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
Mitsubishi Electric CNC M800/M80/E80 series	M800W	BND-2005W000-**	
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	
Mitsubishi Electric CNC M700V/M70V/E70 series	M750VW	BND-1015W002-**	
	M730VW/M720VW	BND-1015W000-**	
	M750VS	BND-1012W002-**	
	M730VS /M720VS	BND-1012W000-**	
	M70V	BND-1018W000-**	
	E70	BND-1022W000-**	

Description

Arbitrary command execution vulnerability due to Missing Authentication for Critical Function (CWE-306)[2] exists in Mitsubishi Electric proprietary protocol communication used in the products listed in the above table.

Impact

A remote attacker may be able to execute arbitrary commands by sending specific packets to the affected products. This could lead to disclose or tamper with information by reading or writing control programs, or cause a denial-of-service (DoS) condition on the products by resetting the memory contents of the products to factory settings or resetting the products remotely.

Countermeasures for Customers

There are no plans to release a fixed version, so we kindly ask you to address this issue through mitigations and 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.
- For MELSEC iQ-F, iQ-R, iQ-L series, and Mitsubishi Electric numerical controller M800V/M80V series and M800/M80/E80 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)
"3.5 Security/IP filter" in the MELSEC iQ-F FX5 Motion Module User's Manual (CC-Link IE TSN)
"1.13 IP Filter" in the MELSEC iQ-R Ethernet User's Manual (Application)
"6.2 Security Function/IP filter" in the MELSEC iQ-R Motion Controller Programming Manual (Common)
"1.4 Security/IP filter" in the MELSEC iQ-R Motion Module User's Manual (Network)
MELSEC iQ-L 运动模块用户手册(网络篇) 1.4 安全 IP 滤波器
"16. Appendix 3 IP Address Filter Setting Function " M800V/M80V Series Instruction Manual
"15. Appendix 2 IP Address Filter Setting Function " M800/M80/E80 Series Instruction Manual

-For Mitsubishi Electric numerical controller M800V/M80V series and M800/M80/E80 series, set the parameter "#11094 GX Restriction" to 1 and limit the operation level of the maintenance screen. For details, please refer to the following manual for each product.

"15 Machine Parameters" M800V/M80V Series Alarm/Parameter Manual
"15 Machine Parameters" M800/M80/E80 Series Alarm/Parameter Manual
"2.8 Changing the Operation Level (Protect Setting Screen)" M800V/M80V Series Instruction Manual
"2.11 Changing the Operation Level (Protect Setting Screen)" M800/M80/E80 Series Instruction Manual

[2] https://cwe.mitre.org/data/definitions/306.html

Contact information

Please contact your local Mitsubishi Electric representative.
<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html

Update history

November 12, 2024

Revised "Title," "Overview," "CVSS," "Description," and "Impact."

Added the following products to the "How to Check the Relevant Products" section.

FX3U-xMy/ES-A (x=16,32,48,64,80,128, y=T,R),FX3UC-16MT/D-P4, FX3UC-16MT/DSS-P4,FX3G-xMy/ES-A (x=14,24,40,60, y=T,R),FX3GE-xMy/z (x=24,40, y=T,R, z=ES,ESS,DS,DSS),FX3GA-xMy-CM (x=24,40,60, y=T,R), FX3SA-xMy-CM (x=10,14,20,30, y=T,R),FX5UJ-xMy/ES-A (x=24,40,60,y=T,R),FX5-xSSC-G x=40,80, FX5-xSSC-S x=40,80,R04/08/16/32/120(EN)CPU,R08/16/32/120PCPU,R16/32/64MTCPU,RD78G4/8/16/32/64/HV/HW, RD77MS2/4/8/16,RD77GF4/8/16/32,LD78G4/16,Q172/173DSCPU,Q170MSCPU,QD77MS2/4/16,QD77GF4/8/16, LD77MS2/4/16, M800VW,M800VS,M80V,M80VW,M800W,M800S,M80,M80W,E80,M750VW,M730VW/M720VW,M750VS,M730VS /M720VS,M70V,E70

Revised "Countermeasure" to "Countermeasures for Customers".