Multiple Denial-of-Service Vulnerabilities in Ethernet port of MELSEC and MELIPC Series

Release date: November 30, 2021
Mitsubishi Electric Corporation

■Overview

Multiple Denial-of-Service (DoS) vulnerabilities exist in MELSEC iQ-R/Q/L series CPU module and MELIPC series. A remote attacker may stop the program execution or Ethernet communication of the products by sending specially crafted packets. (CVE-2021-20609, CVE-2021-20610, CVE-2021-20611)

■CVSS

・CVE-2021-20609 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
・CVE-2021-20610 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
・CVE-2021-20611 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

■Affected products

Affected product model name, firmware version and serial No. are the followings.

Series		Model name	Version
MELSEC	iQ-R Series	R00/01/02CPU	Firmware versions "24" and prior*1
		R04/08/16/32/120(EN)CPU	Firmware versions "57" and prior*1
		R08/16/32/120SFCPU	All versions
		R08/16/32/120PCPU	Firmware versions "29" and prior*1
		R08/16/32/120PSFCPU	All versions
		R16/32/64MTCPU	All versions
		R12CCPU-V	All versions
	Q Series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU	All versions
		Q03/04/06/13/26UDVCPU	The first 5 digits of serial No. "23071" and prior*2
		Q04/06/13/26UDPVCPU	The first 5 digits of serial No. "23071" and prior*2
		Q12DCCPU-V, Q24DHCCPU-V(G), Q24/26DHCCPU-LS	All versions
		MR-MQ100	All versions
		Q172/173DCPU-S1, Q172/172DSCPU	All versions
		Q170MCPU, Q170MSCPU(-S1)	All versions
	L Series	L02/06/26CPU(-P), L26CPU-(P)BT	All versions
MELIPC Series		MI5122-VW	All versions

Please refer to the following user's manual to check firmware version and serial No..

*1:MELSEC iQ-R Module Configuration Manual "Appendix 1 Checking Production Information and Firmware Version"
*2:QCPU User's Manual (Hardware Design, Maintenance and Inspection) "Appendix 5 Checking Serial Number and Function Version"

■Description

Multiple Denial-of-Service (DoS) vulnerabilities below exist in MELSEC iQ-R/Q/L series CPU module and MELIPC series.

・CVE-2021-20609: Uncontrolled Resource Consumption (CWE-400)
・CVE-2021-20610: Improper Handling of Length Parameter Inconsistency (CWE-130)
・CVE-2021-20611: Improper Input Validation (CWE-20)

■Impact

A remote attacker may stop the program execution or Ethernet communication of the products by sending specially crafted packets. A system reset of the products is required for recovery.

■Countermeasures

The following products have been fixed. Mitsubishi Electric will fix other products in the near future.

Series	Model name	Version
iQ-R Series	R00/01/02CPU	Firmware versions "25" or later
	R04/08/16/32/120(EN)CPU	Firmware versions "58" or later
	R08/16/32/120PCPU	Firmware versions "30" or later
Q Series	Q03/04/06/13/26UDVCPU	The first 5 digits of serial No. "23072" or later
	Q04/06/13/26UDPVCPU	The first 5 digits of serial No. "23072" or later

■Mitigation/Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities:

- 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 the remote password function or IP filter function*3 to block access from untrusted hosts.

*3: For details on the remote password function and IP filter function, please refer to the following manual for each product.

MELSEC iQ-R Ethernet User's Manual (Application) 1.13 Security "Remote password" "IP filter"
MELSEC iQ-R Motion Controller Programming Manual (Common) 6.2 Security Function "IP filter"
MELSEC iQ-R C Controller Module User's Manual (Application) 6.6 Security Function "IP filter"
QnUCPU User's Manual (Communication via Built-in Ethernet Port) "CHAPTER 10 REMOTE PASSWORD"
MELSEC-L CPU Module User's Manual (Built-In Ethernet Function) "CHAPTER 11 REMOTE PASSWORD"
MELIPC MI5000 Series User's Manual (Application) "11.3 IP Filter Function"

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

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