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

Release date: November 30, 2021
Last update date: November 9, 2023
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[1]

・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, serial No. and operating system software version 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	Firmware versions "26" and prior*1
		R08/16/32/120PCPU	Firmware versions "29" and prior*1
		R08/16/32/120PSFCPU	Firmware versions "08" and prior*1
		R16/32/64MTCPU	Operating system software version "23" and prior*6
		R12CCPU-V	Firmware versions "16" and prior*1
	Q Series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU	The first 5 digits of serial No. "23121" and prior*2
		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	The first 5 digits of serial No. "24031" and prior*2
		MR-MQ100	Operating system software version "F" and prior*3
		Q172/173DCPU-S1	Operating system software version "W" and prior*4
		Q172/173DSCPU	Operating system software version "Y" and prior*4
		Q170MCPU	Operating system software version "W" and prior*5
		Q170MSCPU(-S1)	Operating system software version "Y" and prior*8
	L Series	L02/06/26CPU(-P), L26CPU-(P)BT	The first 5 digits of serial No. "23121" and prior*2
MELIPC Series		MI5122-VW	Firmware versions "05" and prior*7

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

*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"
*3:MR-MQ100 User's Manual(Details) "1.3 Combination of software version and a function"
*4:Q173D(S)CPU/Q172D(S)CPU User's Manual "2.2.2 Checking operating system software version"
*5:Q170MCPU User's Manual "2.2.2 Checking operating system software version"
*6:MELSEC iQ-R Motion Controller User's Manual "1.3 Checking Production Information and Operating System Software Version"

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

*7:MELIPC MI5000 Series User's Manual (Startup) "Appendix 17 Checking Production Information and Firmware Version"
*8:Q170MSCPU(-S1) User's Manual "2.2.2 Checking operating system software 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)[2]
- CVE-2021-20610: Improper Handling of Length Parameter Inconsistency (CWE-130)[3]
- CVE-2021-20611: Improper Input Validation (CWE-20)[4]

■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

We have fixed the vulnerability at the following version.

Series		Model name	Version
MELSEC	iQ-R Series	R00/01/02CPU	Firmware versions "25" or later
		R04/08/16/32/120(EN)CPU	Firmware versions "58" or later
		R08/16/32/120SFCPU	Firmware versions "27" or later
		R08/16/32/120PCPU	Firmware versions "30" or later
		R08/16/32/120PSFCPU	Firmware versions "09" or later
		R16/32/64MTCPU	Operating system software version "24" or later
		R12CCPU-V	Firmware versions "17" or later
	Q Series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU	The first 5 digits of serial No. "23122" or later
		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
		Q12DCCPU-V, Q24DHCCPU-V(G), Q24/26DHCCPU-LS	The first 5 digits of serial No. "24032" or later
		MR-MQ100	Operating system software version "G" or later
		Q172/173DCPU-S1	Operating system software version "X" or later
		Q172/173DSCPU	Operating system software version "Z" or later
		Q170MCPU	Operating system software version "X" or later
		Q170MSCPU(-S1)	Operating system software version "Z" or later
	L Series	L02/06/26CPU(-P), L26CPU-(P)BT	The first 5 digits of serial No. "23122" or later
MELIPC Series		MI5122-VW	Firmware versions "06" 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[*9] to block access from untrusted hosts.

*9: 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

2 https://cwe.mitre.org/data/definitions/400.html
3 https://cwe.mitre.org/data/definitions/130.html
4 https://cwe.mitre.org/data/definitions/20.html

■Update history

November 9, 2023

Added modules that have been fixed to “Countermeasures”.
Q172/173DSCPU, Q170MSCPU(-S1)

April 24, 2023

Corrected affected and fixed versions.
R08/16/32/120SFCPU

November 24, 2022

Added modules that have been fixed to “Countermeasures”.
R08/16/32/120SFCPU

July 26, 2022

Added modules that have been fixed to “Countermeasures”.
R12CCPU-V, MI5122-VW

May 31, 2022

Added modules that have been fixed to “Countermeasures”.
R08/16/32/120PSFCPU, R16/32/64MTCPU

April 26, 2022

Added modules that have been fixed to “Countermeasures”.
Q12DCCPU-V, Q24DHCCPU-V(G), Q24/26DHCCPU-LS, MR-MQ100, Q172/173DCPU-S1, Q170MCPU

January27, 2022

Added modules that have been fixed to “Countermeasures”.
Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU, L02/06/26CPU(-P), L26CPU-(P)BT
Corrected product model name of “Affected products”
Q172/173DSCPU