Denial-of-Service Vulnerability
in Ethernet port of MELSEC iQ-R, iQ-L Series and MELIPC Series

Release date: December 22, 2022
Last update date: September 5, 2024
Mitsubishi Electric Corporation

Overview

Denial-of-Service (DoS) vulnerability due to improper resource shutdown or release (CWE-404)[1] exists in MELSEC iQ-R, iQ-L series CPU module and MELIPC series. This vulnerability allows a remote attacker to cause a Denial-of-Service (DoS) condition in Ethernet communication on the module by sending specially crafted packets. (CVE-2022-33324)

CVSS[2]

CVE-2022-33324 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 are the followings.

Series	Model name	Version
MELSEC iQ-R Series	R00/01/02CPU	Firmware versions "32" and prior
	R04/08/16/32/120(EN)CPU	Firmware versions "65" and prior
	R08/16/32/120SFCPU	Firmware versions "29" and prior
	R08/16/32/120PSFCPU	Firmware versions "08" and prior
	R12CCPU-V	Firmware versions "17" and prior
MELSEC iQ-L Series	L04/08/16/32HCPU (*1)	Firmware versions "05" and prior
MELIPC Series	MI5122-VW	Firmware versions "07" and prior

(*1) These products are sold in limited regions.

Please refer to the following manual for how to check the firmware version.
-MELSEC iQ-R Module Configuration Manual "Appendix 1 Checking Production Information and Firmware Version"
-MELSEC iQ-L Module Configuration Manual "Appendix 1 Checking Production Information and Firmware Version"
-MELIPC MI5000 Series User's Manual (Startup) "Appendix 17 Checking Production Information and Firmware Version"
Please download the manual from the following URL.
https://www.mitsubishielectric.com/fa/download/index.html

Description

Denial-of-Service (DoS) vulnerability due to improper resource shutdown or release (CWE-404) exists in MELSEC iQ-R, iQ-L series CPU module and MELIPC series.

Impact

This vulnerability allows a remote attacker to cause a Denial-of-Service (DoS) condition in Ethernet communication on the module by sending specially crafted packets. A system reset of the module is required for recovery.

Countermeasures for Customers

<Customers using the affected models of MELSEC iQ-R series products>
Refer to "Appendix 2 Firmware Update Function" in the MELSEC iQ-R Module Configuration Manual to check if the firmware version of your product is updatable.

- In case your product is updatable
  Download a fixed firmware update file from the following site and update the firmware.
  https://www.mitsubishielectric.com/fa/download/index.html
  Refer to "Appendix 2 Firmware Update Function" in the MELSEC iQ-R Module Configuration Manual for information on how to update the firmware.

- In case your product is not updatable
  Take the following Mitigations / Workarounds.
  We have released the fixed version as shown below, but updating the product to the fixed version is not available.

[1] https://cwe.mitre.org/data/definitions/404.html

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

<Customers using the affected models of MELIPC Series or MELSEC iQ-L Series>
Take the following Mitigations / Workarounds.
We have released the fixed version as shown below, but updating the product to the fixed version is not available.

Countermeasures for Products

The following products have been fixed.

Series	Model name	Version
MELSEC iQ-R Series	R00/01/02CPU	Firmware versions "33" or later
	R04/08/16/32/120(EN)CPU	Firmware versions "66" or later
	R08/16/32/120SFCPU	Firmware versions "30" or later
	R08/16/32/120PSFCPU	Firmware versions "09" or later
	R12CCPU-V	Firmware versions "18" or later
MELSEC iQ-L Series	L04/08/16/32HCPU	Firmware versions "06" or later
MELIPC Series	MI5122-VW	Firmware versions "08" or later

Mitigations / Workarounds

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

- Use a firewall, 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 IP filter function[*2] to block access from untrusted hosts.

[*2] For details on the IP filter function, please refer to the following manual for each product.
MELSEC iQ-R Ethernet User’s Manual (Application) 1.13 Security "IP filter"
MELSEC iQ-L CPU module User’s Manual (Application) 24.1 "IP filter Function"
MELSEC iQ-R C Controller Module User's Manual (Application) 6.6 Security Function "IP filter"
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

Update history

September 5, 2024
Added module that has been fixed to “Affected products” and “Countermeasures for Products”.
R08/16/32/120PSFCPU
Added annotation for L04/08/16/32HCPU in “Affected products”.

July 4, 2024
Revised description regarding the iQ-R series of “Countermeasures for Customers”.
Added description regarding the iQ-L series to “Countermeasures for Customers”.
Added module that has been fixed to “Countermeasures for Products”.
L04/08/16/32HCPU

May 30, 2024
“Countermeasures” divided into “Countermeasures for Customers“ and "Countermeasures for Products".
Revised description regarding “Countermeasures for Customers”.
Added module that has been fixed to “Countermeasures for Products”.
MI5122-VW

December 12, 2023
Added module that has been fixed to “Countermeasures”.
R12CCPU-V

July 13, 2023
Added modules that have been fixed to “Countermeasures”.
R08/16/32/120SFCPU