Denial-of-Service Vulnerability in Ethernet Port on CPU Module of MELSEC iQ-R, Q and L Series

Release date: October 29, 2020
Last update date: September 5, 2024
Mitsubishi Electric Corporation

Overview

Mitsubishi Electric is aware of a denial-of-service (DoS) vulnerability in MELSEC iQ-R, Q and L series CPU modules due to uncontrolled resource consumption. When the CPU module receives a specially crafted packet from a malicious attacker, Ethernet communication may enter a DoS condition. (CVE-2020-5652)
The product models, firmware versions, operating system versions and serial number affected by this vulnerability are listed below.

CVSS[1]

CVE-2020-5652 CVSS:3.0/AV: N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

Affected products

The following MELSEC iQ-R, Q and L series CPU modules are affected:

Series	Model name	Version
iQ-R Series	R00/01/02CPU	firmware versions "20" and prior
	R04/08/16/32/120(EN) CPU	firmware versions "52" and prior
	R08/16/32/120SFCPU	firmware versions "22" and prior
	R08/16/32/120PCPU	firmware versions "24" and prior
	R08/16/32/120PSFCPU	firmware versions "06" and prior
	R16/32/64MTCPU	operating system software versions "21" and prior
Q Series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU	The first 5 digits of serial number "22081" and prior
	Q03/04/06/13/26UDVCPU	The first 5 digits of serial number "22031" and prior
	Q04/06/13/26UDPVCPU	The first 5 digits of serial number "22031" and prior
	Q172/173DCPU-S1	operating system software versions "V" and prior
	Q172/173DSCPU	operating system software versions "W" and prior
	Q170MCPU	operating system software versions "V" and prior
	Q170MSCPU(-S1)	operating system software versions "W" and prior
	MR-MQ100 (*)	operating system software versions "E" and prior
L Series	L02/06/26CPU(-P), L26CPU-(P)BT	The first 5 digits of serial number "23121" and prior

(*) This product is sold in limited regions.

For information on checking the firmware version, the operating system software version or the serial number, please refer to the manual for the affected product.
Please download the manual from the following URL.
https://www.mitsubishielectric.com/fa/download/index.html

Description

A denial-of-service (DoS) vulnerability due to uncontrolled resource consumption (CWE-400)[2] exists in MELSEC iQ-R, Q and L series CPU modules.

Impact

When the CPU module receives a specially crafted packet from a malicious attacker, Ethernet communication function may enter a DoS condition, and a reset is required to recover it.

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/400.html

Countermeasures for Customers

Refer to the table below to check if the version of your product is updatable.

Series	Model name	Update availability
iQ-R Series	R00/01/02CPU	Refer to “Appendix 2 Firmware Update Function” in the MELSEC iQ-R Module Configuration Manual.
	R04/08/16/32/120(EN)CPU	
	R08/16/32/120SFCPU	
	R08/16/32/120PCPU	
	R08/16/32/120PSFCPU	
	R16/32/64MTCPU	Updatable in all versions.
Q Series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU	Not updatable in any version.
	Q03/04/06/13/26UDVCPU	
	Q04/06/13/26UDPVCPU	
	Q172/173DCPU-S1	Updatable in all versions.
	Q172/173DSCPU	
	Q170MCPU	
	Q170MSCPU(-S1)	
	MR-MQ100	
L Series	L02/06/26CPU(-P), L26CPU-(P)BT	Not updatable in any version.

<In case your product is updatable>
Download a fixed update file from the following site and update the firmware or operating system software.
https://www.mitsubishielectric.com/fa/download/index.html
Refer to below for detail on updating.

- “Appendix 2 Firmware Update Function” in the MELSEC iQ-R Module Configuration Manual
- “8.4 Installing the Operating System Software” in the MELSEC iQ-R Motion Controller Programing Manual (Common)
- “5.3 Operating System Software Installation Procedure” in the Q173D(S)/Q172(S)CPU Motion Controller User’s Manual
- “5.3 Operating System Software Installation Procedure” in the Q170MCPU Motion Controller User’s Manual
- “5.3 Operating System Software Installation Procedure” in the Q170MSCPU Motion Controller User’s Manual
- “5.3 Operating System Software Installation Procedure” in the MR-MQ100 Motion Controller User’s Manual (Details)

<In case your product is not updatable>
Take the following Mitigations / Workarounds.
We have released the fixed version as shown in “Countermeasures for Products”, but updating the product to the fixed version is not available.
If you are using the affected MELSEC Q and L series products, please consider switching to the succeeding MELSEC iQ-R series.

Countermeasures for Products

The following modules have been fixed.

Series	Model name	Version
iQ-R Series	R00/01/02CPU	firmware versions "21" or later
	R04/08/16/32/120(EN)CPU	firmware versions "53" or later
	R08/16/32/120SFCPU	firmware versions "23" or later
	R08/16/32/120PCPU	firmware versions "25" or later
	R08/16/32/120PSFCPU	firmware versions "07" or later
	R16/32/64MTCPU	operating system software versions "22" or later
Q Series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU	The first 5 digits of serial number "22082" or later
	Q03/04/06/13/26UDVCPU	The first 5 digits of serial number "22032" or later
	Q04/06/13/26UDPVCPU	The first 5 digits of serial number "22032" or later
	Q172/173DCPU-S1	operating system software versions "W" or later
	Q172/173DSCPU	operating system software versions "X" or later
	Q170MCPU	operating system software versions "W" or later
	Q170MSCPU(-S1)	operating system software versions "X" or later
	MR-MQ100	operating system software versions "F" or later
L Series	L02/06/26CPU(-P), L26CPU-(P)BT	The first 5 digits of serial number "23122" 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 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.

Acknowledgement

Mitsubishi Electric would like to thank joker63 of ZheJiangQiAnTechnology who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.

Update history

September 5, 2024

Added Operating system version and serial number in “Overview”.
“Countermeasures” divided into “Countermeasures for Customers“ and "Countermeasures for Products".
Corrected the firmware version of R 08/16/32/120 PCPU in “Affected products” and “Countermeasures for Products”.
Added R08/16/32/10 PSFCPU in “Affected products” and “Countermeasures for Products”.
Added annotation for MR-MQ100 in “Affected products”.

December 19, 2023

Added the Acknowledgement.

March 29, 2022

Added the information of modules that have been fixed to “Affected products” and “Countermeasures”.

January 13, 2022

Added modules that have been fixed to “Countermeasures”.

May 18, 2021

Added R 08/16/32/120 PCPU that has been fixed to “Countermeasures”.
R 08/16/32/120 PSFCPU has been deleted from “Affected products”.