

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: March 29, 2022
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 and firmware versions affected by this vulnerability are listed below.

■ CVSS

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	R 00/01/02 CPU	firmware versions "20" and prior
	R 04/08/16/32/120 (EN) CPU	firmware versions "52" and prior
	R 08/16/32/120 SFCPU	firmware versions "22" and prior
	R 08/16/32/120 PCPU	firmware versions "25" and prior
	R 16/32/64 MTCPU	operating system software version "21" and prior
Q Series	Q03 UDECPU, Q 04/06/10/13/20/26/50/100 UDEHCPU	serial number "22081" and prior
	Q 03/04/06/13/26 UDVCPU	serial number "22031" and prior
	Q 04/06/13/26 UDPVCPU	serial number "22031" and prior
	Q 172/173 DCPU-S1	operating system software version "V" and prior
	Q 172/173 DSCPU	operating system software version "W" and prior
	Q 170 MCPU	operating system software version "V" and prior
	Q 170 MSCPU(-S1)	operating system software version "W" and prior
	MR-MQ100	operating system software version "E" and prior
L Series	L02/06/26 CPU (-P), L 26 CPU - (P) BT	serial number "23121" and prior

Please check the manual of the affected product for how to check the firmware version, the operating system software version or the serial number.

■ Description

A denial-of-service (DoS) vulnerability due to uncontrolled resource consumption (CWE-400) 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.

■ Countermeasures

The following modules have been fixed.

Series	Model name	Version
iQ-R Series	R 00/01/02 CPU	firmware versions "21" or later
	R 04/08/16/32/120 (EN) CPU	firmware versions "53" or later
	R 08/16/32/120 SFCPU	firmware versions "23" or later
	R 08/16/32/120 PCPU	firmware versions "26" or later
	R 16/32/64 MTCPU	operating system software version "22" or later
Q Series	Q03 UDECPU, Q 04/06/10/13/20/26/50/100 UDEHCPU	serial number "22082" or later
	Q 03/04/06/13/26 UDVCPU	serial number "22032" or later
	Q 04/06/13/26 UDPVCPU	serial number "22032" or later
	Q 172/173 DCPU-S1	operating system software version "W" or later
	Q 172/173 DSCPU	operating system software version "X" or later
	Q 170 MCPU	operating system software version "W" or later
	Q 170 MSCPU(-S1)	operating system software version "X" or later
	MR-MQ100	operating system software version "F" or later
L Series	L02/06/26 CPU (-P), L 26 CPU - (P) BT	serial number "23122" or later

■ Mitigations

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.

■ Contact information

Please contact your local Mitsubishi Electric representative.

■ Update history

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".