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

Release date: October 29, 2020
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 earlier
	R 04/08/16/32/120 (EN) CPU	firmware versions "52" and earlier
	R 08/16/32/120 SFCPU	firmware versions "22" and earlier
	R 08/16/32/120 PCPU	all versions
	R 08/16/32/120 PSFCPU	all versions
	R 16/32/64 MTCPU	all versions
Q Series	Q03 UDECPU, Q 04/06/10/13/20/26/50/100 UDEHCPU	serial number "22081" and earlier
	Q 03/04/06/13/26 UDVCPU	serial number "22031" and earlier
	Q 04/06/13/26 UDPVCPU	serial number "22031" and earlier
	Q 172/173 DCPU-S1	all versions
	Q 172/173 DSCPU	all versions
	Q 170 MCPU	all versions
	Q 170 MSCPU(-S1)	all versions
	MR-MQ100	all versions
L Series	L 02/06/26 CPU (-P), L 26 CPU - (P) BT	all versions

Please check the manual of the affected product for how to check the firmware 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
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

Modules other than above are scheduled to be fixed soon.

■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.