

# Denial-of-Service Vulnerability in Ethernet Port of MELSEC and MELIPC Series

Release date: June 14, 2022

Last update date: August 16, 2022

Mitsubishi Electric Corporation

## ■ Overview

Denial of Service(DoS) vulnerability due to improper resource locking (failure to release resources) exists in MELSEC iQ-R/Q/L series CPU module and MELIPC series. A malicious attacker may cause a DoS condition in Ethernet communications by sending a specially crafted packet (CVE-2022-24946).

The product models and versions affected by this vulnerability are listed below.

## ■ CVSS

CVE-2022-24946 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 and serial No. are the followings.

Series		Model name	Version
MELSEC	iQ-R Series	R12CCPU-V	Firmware versions "16" and prior
	Q Series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU	The first 5 digits of serial No. "24061"and prior
		Q03/04/06/13/26UDVCPU	The first 5 digits of serial No. "24051"and prior
		Q04/06/13/26UDPVCPU	The first 5 digits of serial No. "24051"and prior
		Q12DCCPU-V, Q24DHCCPU-V(G), Q24/26DHCCPU-LS	All versions
	L Series	L02/06/26CPU-(P), L26CPU-(P)BT	The first 5 digits of serial No. "24051"and prior
MELIPC Series		MI5122-VW	Firmware versions "05" and prior

Please refer to the following user's manual for how to check firmware version and serial No..

- MELSEC iQ-R Module Configuration Manual "Appendix 1 Checking Production Information and Firmware Version"
- QCPU User's Manual (Hardware Design, Maintenance and Inspection) "Appendix 5 Checking Serial Number and Function Version"
- MELSEC-L CPU Module User's Manual (Hardware Design, Maintenance and Inspection) "Appendix 5 Checking Serial Number and Function Version"
- MELIPC MI5000 Series User's Manual (Startup) "Appendix 17 Checking Production Information and Firmware Version"

## ■ Description

Denial of Service(DoS) vulnerability due to Improper Resource Locking (CWE-413) exists in MELSEC iQ-R/Q/L series CPU module and MELIPC series.

## ■ Impact

A malicious attacker may cause a DoS condition in Ethernet communications by sending a specially crafted packet (CVE-2022-24946). A system reset of the products is required for recovery.

## ■ Countermeasures

The following modules have been fixed.

Series		Model name	Version
MELSEC	iQ-R Series	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. "24062"or later
		Q03/04/06/13/26UDVCPU	The first 5 digits of serial No. "24052"or later
		Q04/06/13/26UDPVCPU	The first 5 digits of serial No. "24052"or later
	L Series	L02/06/26CPU-(P), L26CPU-(P)BT	The first 5 digits of serial No. "24052"or later
MELIPC Series		MI5122-VW	Firmware versions "06" or later

Other modules will be fixed in the near future.

## ■ Mitigation/Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting the 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.

< Inquiries | MITSUBISHI ELECTRIC FA >

<https://www.mitsubishielectric.com/fa/support/index.html>

#### ■ Update history

August 16, 2022

The title has been changed due to the addition of affected products.

Added modules(R12CCPU-V, Q12DCCPU-V, Q24DHCCPU-V (G), Q24/26DHCCPU-LS, MI5122-VW) to "Affected products".

Added modules(R12CCPU-V, Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU, MI5122-VW) that have been fixed to "Countermeasures".