

# Information Disclosure Vulnerability in MELSEC iQ-R Series Safety CPU and SIL2 Process CPU Module

Release date: February 13, 2024  
Last update date: May 16, 2024  
Mitsubishi Electric Corporation

## Overview

Information disclosure vulnerability due to Incorrect Privilege Assignment (CWE-266<sup>1</sup>) exists in MELSEC iQ-R Series Safety CPU and SIL2 Process CPU modules. After a remote attacker logs into the CPU module as a non-administrator user, the attacker may disclose the credentials (user ID and password) of a user with a lower access level than the attacker by sending a specially crafted packet. (CVE-2023-6815)

## CVSS<sup>2</sup>

CVE-2023-6815 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N Base Score : 6.5

## Affected products

The following products and firmware versions are affected:

Series	Product name	Firmware Version
MELSEC iQ-R Series Safety CPU	R08/16/32/120SF CPU	all versions
MELSEC iQ-R Series SIL2 Process CPU	R08/16/32/120PSF CPU	all versions

## Description

Information disclosure vulnerability due to Incorrect Privilege Assignment (CWE-266) exists in MELSEC iQ-R Series Safety CPU and SIL2 Process CPU modules.

## Impact

After a remote attacker logs into the CPU module as a non-administrator user, the attacker may disclose the credentials (user ID and password) of a user with a lower access level than the attacker by sending a specially crafted packet.

## Countermeasures for Customers

Customers using the affected products and firmware versions may take the following measures:

Series	Product name	Firmware Version	Countermeasures
MELSEC iQ-R Series Safety CPU	R08/16/32/120SF CPU	"26" and prior	Take measures listed in "Mitigations" section below because updating the product to the enhanced version of vulnerability management is not available.
		"27" or later	Take measures described in "Workarounds" section.
MELSEC iQ-R Series SIL2 Process CPU	R08/16/32/120PSF CPU	"11" and prior	Take measures listed in "Mitigations" section below because updating the product to the enhanced version of vulnerability management is not available.
		"12" or later	Take measures described in "Workarounds" section.

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"

Please download the manual from the following URL.

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

## Workarounds

In the combination of the versions of CPU module and the versions of GX Works3 shown in the following table, an attack against this vulnerability can be prevented by enabling "communicating with only the enhanced version of vulnerability management of GX Works3" (Refer to Figure 1 and 2) when writing user information to the CPU module.

Series	Version of CPU module	Version of GX Works3
MELSEC iQ-R Series Safety CPU	27 or later	1.087R or later
MELSEC iQ-R Series SIL2 Process CPU	12 or later	1.105K or later

<sup>1</sup> <https://cwe.mitre.org/data/definitions/266.html>

<sup>2</sup> <https://www.first.org/cvss/v3.1/specification-document>

[Selection screen for user information writing]

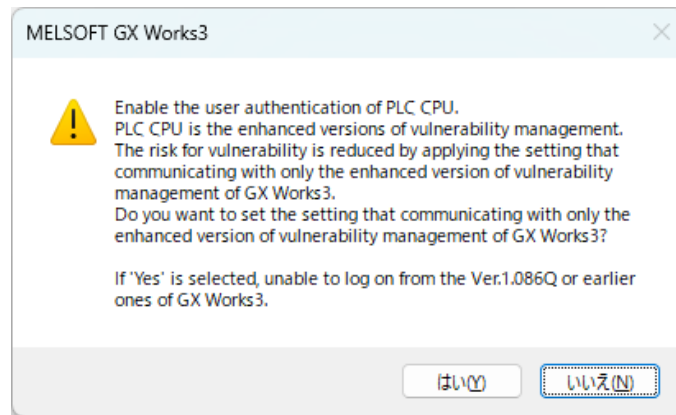


Figure 1 When using MELSEC iQ-R Series Safety CPU

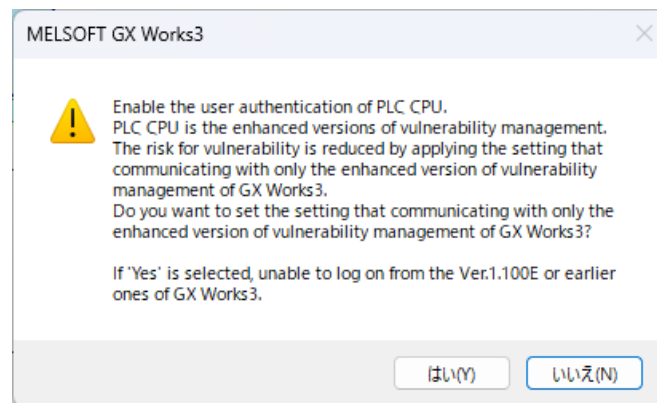


Figure 2 When using MELSEC iQ-R Series SIL2 Process CPU

## 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.
- Use IP filter function\* to block access from untrusted hosts.

\*: For details on the IP filter function, please refer to the following manual for each product.

"1.13 Security" - "IP filter" in the MELSEC iQ-R Ethernet User's Manual(Application)

- Restrict physical access to the affected product as well as to the personal computers and the network devices that can communicate with it.
- Install antivirus software on your personal computer that can access the affected product.

## Acknowledgement

Mitsubishi Electric would like to thank Reid Wightman, Dragos Inc. who reported this vulnerability.

## Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>

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

## Update history

May 16, 2024

Changed from "Countermeasures" to "Countermeasures for Customers" and added countermeasures for customers.

Added modules that have been fixed to "Workarounds".

R08/16/32/120PSFCPU