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

Release date: February 13, 2024
Mitsubishi Electric Corporation

Overview

Information disclosure vulnerability due to Incorrect Privilege Assignment (CWE-266[1]) 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 attcker by sending a specially crafted packet. (CVE-2023-6815)

CVSS[2]

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	R08/16/32/120SFCPU	all versions
MELSEC iQ-R Series SIL2 Process CPU	R08/16/32/120PSFCPU	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

Please carry out the following workarounds.

Workarounds

In the combination of the versions of CPU module and the versions of GX Works3 shown in the following table, this attack can be prevented by enabling "communicating with only the enhanced version of vulnerability management of GX Works3" (Refer to Figure 1) when writing user information to the CPU module.
Mitsubishi Electric will implement the workaround in other products in the near future.

Series	Version of CPU module	Version of GX Works3
MELSEC iQ-R Series Safety CPU	27 or later	1.087R or later

Please contact your local Mitsubishi Electric representative to change to a CPU module of the above version or later.

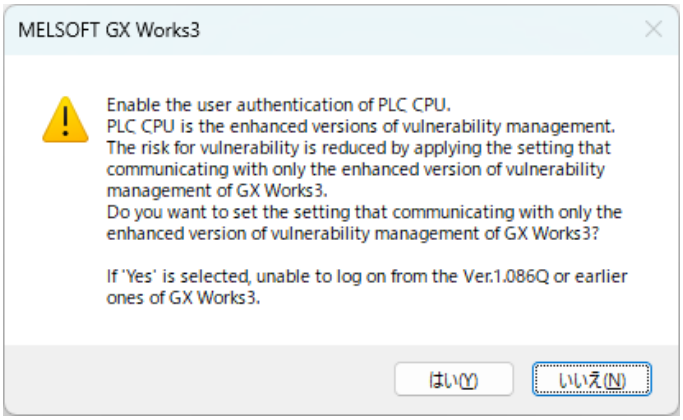

Figure 1 Selection screen for user information writing

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

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

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