Unauthorized login vulnerability in MELSEC iQ-R Series CPU Module

Release date: August 5, 2021
Last update date: April 18, 2024
Mitsubishi Electric Corporation

Overview

An unauthorized login vulnerability exists in MELSEC iQ-R series CPU modules due to Insufficiently Protected Credentials (CWE-522)[1]. A remote attacker could be able to login to the CPU module unauthorizedly by sniffing network traffic and obtaining credentials (CVE-2021-20597).
The product models and firmware versions affected by this vulnerability are listed below.

CVSS[2]

CVE-2021-20597 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N Base Score:7.4

Affected products

The following modules are affected:

Product name	Model name	Firmware Version
MELSEC iQ-R series Safety CPU	R08/16/32/120SFCPU	Firmware versions "26" and prior
MELSEC iQ-R series SIL2 Process CPU	R08/16/32/120PSFCPU	Firmware versions "11" and prior

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

Description

An unauthorized login vulnerability due to Insufficiently Protected Credentials(CWE-522) exists in MELSEC iQ-R series CPU modules.

Impact

When registering user information in the CPU module or changing the password, a remote attacker can sniff network traffic and obtain the credentials, and could be able to login to the CPU module unauthorizedly.

Countermeasures for Customers

Customers using the affected products and versions may take measures through mitigations and workarounds.
We have released the fixed version as shown below, but updating the product to the fixed version is not available.

Countermeasures for Products

The following products have been fixed.

Product name	Model name	Firmware Version
MELSEC iQ-R series Safety CPU	R08/16/32/120SFCPU	Firmware versions "27" or later
MELSEC iQ-R series SIL2 Process CPU	R08/16/32/120PSFCPU	Firmware versions "12" or later

Mitigations / Workarounds

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 the IP filter function*1 to restrict the accessible IP addresses.
- Register user information or change the password via USB. If you have already registered user information or changed the user's

1 https://cwe.mitre.org/data/definitions/522.html
2 https://www.first.org/cvss/v3.1/specification-document

password via the network, change the password once via USB.

*1：MELSEC iQ-R Ethernet User’s Manual(Application) 1.13 Security “IP filter”

Acknowledgement

Mitsubishi Electric would like to thank Ivan Speziale of Nozomi Networks Labs 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

April 18, 2024

Added a firmware version verification method.

“Countermeasures” devided into “Countermeasures for Customers“ and "Countermeasures for Products".

Added modules that have been fixed to “Countermeasures for Products”.

R08/16/32/120PSFCPU

October 13, 2022

Added modules that have been fixed to “Countermeasures”.

R08/16/32/120SFCPU