Authentication Bypass vulnerability in MELSEC iQ-R Series Safety CPU/SIL2 Process CPU Module

Release date: August 6, 2021
Last update date: April 18, 2024
Mitsubishi Electric Corporation

Overview

Cleartext Transmission of Sensitive Information (CWE-319[1]) vulnerability exists in MELSEC iQ-R series Safety CPU/SIL2 Process CPU modules. An unauthenticated remote attacker may be able to login to the CPU module by obtaining credentials other than password. (CVE-2021-20599)

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

CVSS[2]

CVE-2021-20599 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N Base Score:9.1

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

Cleartext transmission of sensitive information vulnerability exists in MELSEC iQ-R series Safety CPU/SIL2 Process CPU modules.

Impact

An unauthenticated remote attacker can obtain the credentials other than password and login to the CPU module.

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.
  *1:MELSEC iQ-R Ethernet User's Manual(Application) 1.13 Security "IP filter"

Acknowledgement

Mitsubishi Electric would like to thank Ivan Speziale, security research of Nozomi Networks who reported this vulnerability.

1 https://cwe.mitre.org/data/definitions/319.html
2 https://www.first.org/cvss/v3.1/specification-document

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
Title changed.
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
Vulnerability Type (CWE) was changed to Cleartext transmission of sensitive information (CWE-319)

October 13, 2021
Correction of clerical errors.

October 12, 2021
Added CVE ID and CVSS score.
Modified part of descriptions of “Overview”, “Description”, “Impact” and “Countermeasures”.