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

Release date: August 6, 2021
Last update date: October 13, 2022
Mitsubishi Electric Corporation

■Overview

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

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	all version

■Description

Cleartext transmission of sensitive information vulnerability (CWE-319) exists in MELSEC iQ-R series Safety CPU/SIL2 Process modules.

■Impact

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

■Countermeasures

The following products have been fixed. Mitsubishi Electric will fix other products in the near future.

Product name	Model name	Firmware Version
MELSEC iQ-R series Safety CPU	R08/16/32/120SFCPU	Firmware versions "27" 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.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

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

■Update history

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”.