Information disclosure vulnerability in MELSEC iQ-R Series CPU Module

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

Overview

An information disclosure vulnerability exists in MELSEC iQ-R Series CPU module due to Exposure of Sensitive Information to an Unauthorized Actor (CWE-200)[1]. A remote attacker can aquire legitimate user names regisiterd in the module by brute-force attack on user names.
The product models and firmware versions affected by this vulnerability are listed below.

CVSS[2]

CVE-2021-20594 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score:5.9

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 information disclosure vulnerability due to Exposure of Sensitive Information to an Unauthorized Actor (CWE-200) exists in MELSEC iQ-R Series CPU module.

Impact

A remote attacker can aquire legitimate user names regisiterd in the module by brute-force attack on user names. However, it is only possible to log-in to the unit, providing that the attacker can aquire the password. Therefore it is not possible to log-in imidiately, even if iligal legitimate user name acquisition is succeeded.

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 either or a combination of 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 https://cwe.mitre.org/data/definitions/200.html
2 https://www.first.org/cvss/v3.1/specification-document

*1：MELSEC iQ-R Ethernet User’s Manual(Application) 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