

Information disclosure vulnerability in MELSEC iQ-R Series CPU Module

Release date: August 5, 2021

Last update date: October 13, 2022

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). A remote attacker can acquire legitimate user names registered in the module by brute-force attack on user names.

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

■ CVSS

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	R08/16/32/120SF CPU	Firmware versions "26" and prior
MELSEC iQ-R series SIL2 Process CPU	R08/16/32/120PSF CPU	all versions

■ 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 acquire legitimate user names registered 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 acquire the password. Therefore it is not possible to log-in immediately, even if illegal legitimate user name acquisition is succeeded.

■ 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	R08/16/32/120SF CPU	Firmware versions "27" 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: 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

October 13, 2022

Added modules that have been fixed to "Countermeasures".

R08/16/32/120SF CPU