Denial-of-Service Vulnerability in MELSEC iQ-R Series Ethernet Port

Release date: October 8, 2020
Last update date: August 22, 2024
Mitsubishi Electric Corporation

Overview

Mitsubishi Electric is aware of a denial-of-service (DoS) vulnerability in MELSEC iQ-R series modules due to uncontrolled resource consumption. When the CPU module receives a specially crafted packet from a malicious attacker, an error may occur on the CPU module and then the program execution and communication may enter a DoS condition. (CVE-2020-16850)
The product models, firmware versions and operating system software versions affected by this vulnerability are listed below.

CVSS[1]

CVE-2020-16850 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H Base Score:8.6

Affected products

The following MELSEC iQ-R series modules are affected:

- R00/01/02CPU : Firmware versions "20" and prior
- R04/08/16/32/120CPU, R04/08/16/32/120ENCPU : Firmware versions "52" and prior
- R08/16/32/120SFCPU : Firmware versions "22" and prior
- R08/16/32/120PCPU : Firmware versions "25" and prior
- R16/32/64MTCPU : Operating system software versions "21" and prior

Please refer to the following manuals for how to check the firmware versions or operating system software versions.

- "Appendix 1 Checking Production Information and Firmware Version" in the MELSEC iQ-R Module Configuration Manual
- "1.3 Checking Production Information and Operating System Software Version" in the MELSEC iQ-R Motion Controller User's Manual

Please download the manual from the following URL.
https://www.mitsubishielectric.com/fa/download/index.html

Description

A denial-of-service (DoS) vulnerability due to uncontrolled resource consumption (CWE-400)[2] exists in MELSEC iQ-R series modules.

Impact

When the CPU module receives a specially crafted packet from a malicious attacker, an error may occur on the CPU module and then the program execution and communication may enter a DoS condition, and a reset is required to recover it.

Countermeasures for Customers

Refer to the table below to check if the version of your product is updatable.

Series	Model name	Update availability
iQ-R series	R00/01/02CPU	Refer to "Appendix 2 Firmware Update Function" in the MELSEC iQ-R Module Configuration Manual.
	R04/08/16/32/120CPU, R04/08/16/32/120ENCPU	
	R08/16/32/120SFCPU	
	R08/16/32/120PCPU	
	R16/32/64MTCPU	Updatable in all versions.

<In case your product is updatable>
Download a update file for the fixed version from the following site and update the firmware or operating system software.
https://www.mitsubishielectric.com/fa/download/index.html
Refer to below for detail on updating.

- "Appendix 2 Firmware Update Function" in the MELSE iQ-R Module Configuration Manual
- "8.4 Installing the Operating System Software" in the MELSEC iQ-R Motion Controller Programing Manual (Common)

<In case your product is not updatable>
Take the following Mitigations / Workarounds.
We have released the fixed version as shown in "Countermeasures for Products", but updating the product to the fixed version is not

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/400.html

available.

Countermeasures for Products

The following modules have been fixed.

- R00/01/02CPU : Firmware versions “21” or later
- R04/08/16/32/120CPU, R04/08/16/32/120ENCPU : Firmware versions “53” or later
- R08/16/32/120SFCPU : Firmware versions “23” or later
- R08/16/32/120PCPU : Firmware versions “26” or later
- R16/32/64MTCPU : Operating system software versions “22” 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 though firewalls.

Acknowledgement

Mitsubishi Electric would like to thank Yossi Reuven of SCADAfence Ltd. who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTIRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html

Update history

August 22, 2024

Deleted R08/16/32/120PFSCPU from “Affected products” and “Countermeasures”.
Added the “CVSS”.
“Countermeasures” divided into “Countermeasures for Customers“ and "Countermeasures for Products".
Added the operating system software version in the “Overview”
Corrected the firmware versions to operating system software versions in the “Affected products” and “Countermeasures for Products”.

May 18, 2021

Added affected product (R 08/16/32/120 PSFCPU). Added R 16/32/64 MTCPU that has been fixed to “Countermeasures”.

February 18, 2021

Added modules that have been fixed to “Countermeasures”.

October 26, 2020

Added modules that have been fixed to “Countermeasures”.