Denial-of-Service Vulnerability in MELSEC iQ-R Series CPU Modules

Release date: November 12, 2020
Mitsubishi Electric Corporation

■Overview

Mitsubishi Electric is aware of a denial-of-service (DoS) vulnerability in MELSEC iQ-R series CPU modules due to uncontrolled resource consumption. CPU modules allow malicious attacker to cause a DoS by sending specially crafted http packets. (CVE-2020-5666)

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

■CVSS

CVE-2020-5666 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H Base Score:6.8

■Affected products

The following MELSEC iQ-R series CPU modules are affected:

・R00/01/02CPU：Firmware versions from "05" to "19"
・R04/08/16/32/120(EN)CPU：Firmware versions from "35" to "51"

The firmware version of the CPU module can be checked on the following "Product Information List(Fig 1)" window of system monitor in GX Works3.

For details, refer to the following section in the manual.

・MELSEC iQ-R Module Configuration Manual (Appendix 1 Checking Production Information and Firmware Version)

	Network Information (Port 2)	IP Address (Port1 IPv4)	IP Address (Port2 IPv4)	Module Synchronous Status	Firmware Version	Production information
Basic-Power Supply	-	-	-	-	-	-
Basic-CPU	-	-	-	-	51	-
Basic-I/O 0	-	-	-	-	-	-
Basic-I/O 1	-	-	-	-	-	-
Basic-I/O 2	-	-	-	-	-	-
Basic-I/O 3	-	-	-	-	-	-
Basic-I/O 4	-	-	-	-	-	-
Basic-I/O 5	-	-	-	-	-	-
Basic-I/O 6	-	-	-	-	-	-
Basic-I/O 7	-	-	-	-	-	-

Fig 1 Product Information List

■Description

A denial-of-service (DoS) vulnerability due to uncontrolled resource consumption (CWE-400) exists in MELSEC iQ-R series CPU modules. In case of "To Use or Not to Use Web Server Settings" in the parameter of CPU modules are set to "Not Use", this phenomenon does not occur. (The default setting is "Not Use".)

■Impact

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

■Countermeasures

This issue is fixed in following firmware versions.

・R00/01/02CPU：firmware versions "20" or later
・R04/08/16/32/120(EN)CPU：firmware versions "52" or later

■Mitigations

– If Web Server function is not need, set "Not Use" for "To Use or Not to Use Web Server Settings". Check the following for the setting method

[The setting method]

Web server setting can be configured as follows(Fig 2):

① [Parameter]–[CPU module]–[Module Parameter]–[Application Settings]–[Web Server Settings]

② Set "Not Use" for "To Use or Not to Use Web Server Settings"

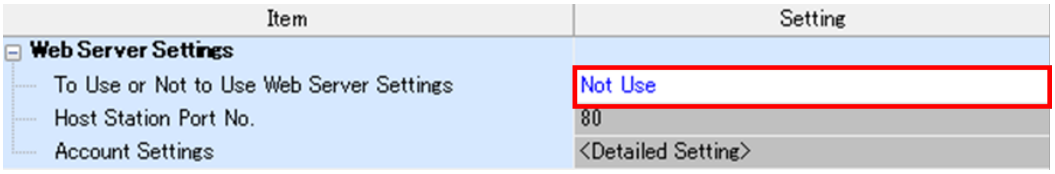

Fig 2 Web Server Settings

And, Mitsubishi Electric recommends that customers take following mitigations 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 trusted LAN and block access from untrusted networks and hosts through firewalls.

■Acknowledgement

Mitsubishi Electric would like to thank Xiaofei.Zhang of China Industrial Control Systems Cyber Emergency Response Team who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.