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

Release date: June 9, 2020
Last update date: November 5, 2020
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 (CWE-400). When an attacker sends a large amount of specially crafted packets in burst over a short period of time, the Ethernet port may enter a DoS condition.

* The DoS (Denial-of-Service) condition means the condition that an attacker interferes with the corresponding service.

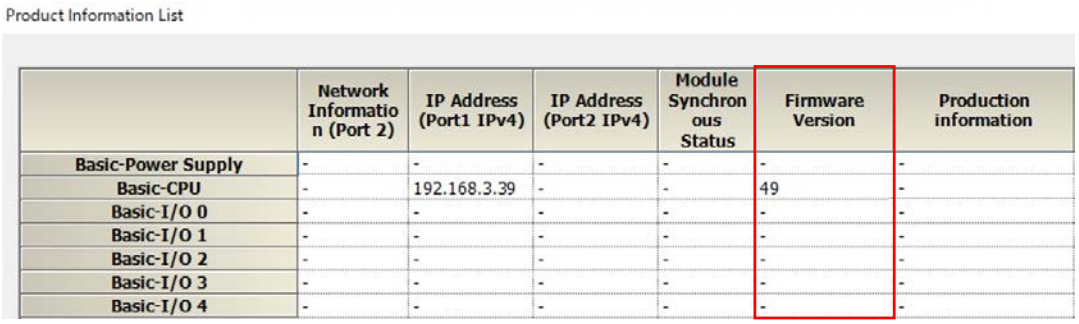
■Affected products

The following products are affected.

・R00/01/02CPU: firmware versions "7" or earlier
・R04/08/16/32/120CPU, R04/08/16/32/120ENCPU: firmware versions "39" or earlier
・R08/16/32/120SFCPU: firmware versions "20" or earlier
・R08/16/32/120PCPU: firmware versions "24" or earlier
・R08/16/32/120PSFCPU: firmware versions "05" or earlier
・RJ71EN71: firmware versions "49" or earlier

The firmware version of the module can be checked on the following "Product Information List" window of system monitor in GX Works3.
For how to check firmware version, please refer to the following manual.
・MELSEC iQ-R Module Configuration Manual (Appendix 1 Checking Production Information and Firmware Version)

[Product Information List]


Product Information List

	Network Information (Port 2)	IP Address (Port1 IPv4)	IP Address (Port2 IPv4)	Module Synchronous Status	Firmware Version	Production information
Basic-Power Supply	-	-	-	-	-	-
Basic-CPU	-	192.168.3.39	-	-	49	-
Basic-I/O 0	-	-	-	-	-	-
Basic-I/O 1	-	-	-	-	-	-
Basic-I/O 2	-	-	-	-	-	-
Basic-I/O 3	-	-	-	-	-	-
Basic-I/O 4	-	-	-	-	-	-

■Description

A denial-of-service (DoS) vulnerability (CVE-2020-13238) due to uncontrolled resource consumption (CWE-400) exists in MELSEC iQ-R series modules.

■Impact

When an attacker sends a large amount of specially crafted packets in burst over a short period of time, the Ethernet port may enter a DoS condition.

■Countermeasures

The following modules have been fixed to discard packets when specially crafted packets are received.

・R00/01/02CPU: firmware versions "8" or later
・R04/08/16/32/120CPU, R04/08/16/32/120ENCPU: firmware versions "40" or later
・R08/16/32/120SFCPU: firmware versions "21" or later
・R08/16/32/120PCPU: firmware versions "25" or later
・R08/16/32/120PSFCPU: firmware versions "06" or later
・RJ71EN71: firmware versions "50" or later

■Mitigations

For cyber-attacks such as DoS attack or unauthorized access from untrusted networks or hosts, the following measures need to be taken by users.

1. Checking for connection to untrusted networks or hosts
   Please check whether the modules mounted in the equipment you are using are connected to untrusted networks or hosts.
2. Checking for firewalls
   If the modules are connected to untrusted networks or hosts, please check whether measures such as firewalls are taken.

For whether the modules used are connected to untrusted networks or hosts, or whether measures such as firewalls are taken, please contact your IT department or local supplier.

■Acknowledgements

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

■Contact information

For inquiries, please contact your local Mitsubishi Electric representative.

■Update history

November 5, 2020

Added modules that have been fixed to “Countermeasures”.