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

Release date: November 19, 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. When a module receives a specially crafted SLMP packet from a malicious attacker, the program execution and communication may enter a DoS condition (CVE-2020-5668).
The product models and firmware versions affected by this vulnerability are listed below.

■CVSS

CVE-2020-5668 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

■Affected products

The following MELSEC iQ-R series modules are affected:

Series	Model name	Version
iQ-R series	R00/01/02CPU	firmware versions "19" and earlier
	R04/08/16/32/120(EN)CPU	firmware versions "51" and earlier
	R08/16/32/120SFCPU	firmware versions "22" and earlier
	R08/16/32/120PCPU	all versions
	R08/16/32/120PSFCPU	all versions
	RJ71EN71	firmware versions "47" and earlier
	RJ71GF11-T2	firmware versions "47" and earlier
	RJ72GF15-T2	firmware versions "07" and earlier
	RJ71GP21-SX	firmware versions "47" and earlier
	RJ71GP21S-SX	firmware versions "47" and earlier
	RJ71C24(-R2/R4)	all versions
	RJ71GN11-T2	all versions

The firmware version of the module can be checked on the following "Product Information List(Fig 1)" window of system monitor in GX Works3.
Please check the manual of the affected product for how to check.

	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 modules.

■Impact

When a module receives a specially crafted SLMP packet from a malicious attacker, the module may enter the following condition. To recover it, a reset is required.

① CPU module
An error may occur on the CPU module then the program execution and communication may enter a DoS condition.

② Other than CPU module
Communication via the module may enter a DoS condition.

■Countermeasures

The following modules have been fixed.

Series	Model name	Version
iQ-R Series	R00/01/02CPU	firmware versions "20" or later
	R04/08/16/32/120(EN)CPU	firmware versions "52" or later
	R08/16/32/120SFCPU	firmware versions "23" or later
	RJ71EN71	firmware versions "48" or later
	RJ71GF11-T2	firmware versions "48" or later
	RJ72GF15-T2	firmware versions "08" or later
	RJ71GP21-SX	firmware versions "48" or later
	RJ71GP21S-SX	firmware versions "48" or later

Modules other than above are scheduled to be fixed soon.

■Mitigations

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 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.