

TECHNICAL BULLETIN

[1 / 4]

FA-A-0313-A

Vulnerabilities of MELSEC iQ-R Series Modules with an Ethernet Port

■Date of Issue

July 2020

■Relevant Models

Rn(EN)CPU, RnSF CPU, RnP(SF)CPU, RJ71EN71

Thank you for your continued support of Mitsubishi Electric programmable controllers, MELSEC iQ-R series.

Vulnerabilities in the MELSEC iQ-R series modules with an Ethernet port^{*1} have been clarified. We will inform you of the overview of vulnerabilities and the measures that must be taken by users.

*1 Modules with an Ethernet connector

1 RELEVANT MODELS

The following table lists the products that have vulnerabilities.

Product	Model	Firmware version ^{*1}
Programmable controller CPU	R00CPU, R01CPU, R02CPU	07 or earlier
	R04CPU, R08CPU, R16CPU, R32CPU, R120CPU, R04ENCPU, R08ENCPU, R16ENCPU, R32ENCPU, R120ENCPU	39 or earlier
Safety CPU	R08SFPCPU, R16SFPCPU, R32SFPCPU, R120SFPCPU	20 or earlier
Process CPU	R08PCPU, R16PCPU, R32PCPU, R120PCPU	All versions
SIL2 process CPU	R08PSFPCPU, R16PSFPCPU, R32PSFPCPU, R120PSFPCPU	All versions
Ethernet module	RJ71EN71	All versions

*1 After updating firmware, check the version.



Check the firmware version on the system monitor of an engineering tool.
For checking procedure details, refer to the MELSEC iQ-R Module Configuration Manual.

2 IMPACT

If a MELSEC iQ-R series module with an Ethernet port receives a large number of packets camouflaged by attackers in a short time, Ethernet communication may be interrupted.

For details, refer to the following.


Website	URL
ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)	us-cert.cisa.gov/ics/advisories/icsa-20-161-02
JPCERT (Japan Computer Emergency Response Team)	jvn.jp/vu/JVNVU97662844/

3 MEASURES

3.1 Measures for Modules

To strengthen security, continued Ethernet communication support is available for the following module versions.

Product	Model	Firmware version
Programmable controller CPU	R00CPU, R01CPU, R02CPU	08 or later
	R04CPU, R08CPU, R16CPU, R32CPU, R120CPU, R04ENCPU, R08ENCPU, R16ENCPU, R32ENCPU, R120ENCPU	40 or later
Safety CPU	R08SFCPU, R16SFCPU, R32SFCPU, R120SFCPU	21 or later

Changes are planned for the future for modules other than the modules listed above. Refer to  Page 3 Measures Taken by Users.

3.2 Measures Taken by Users

Take measures such as installing a firewall to prevent unauthorized access via networks.

Contact your IT department or local supplier whether your modules are connected to networks or not, and whether measures such as firewalls are taken or not.

Item	Description
Checking for network connection	Check whether the modules installed on any used equipment are connected to networks or not.
Checking for firewalls	Block access from communications via untrusted networks and hosts using firewalls.

FA-A-0313-A

REVISIONS

Version	Date of Issue	Revision
A	July 2020	First edition

TRADEMARKS

The company names, system names and product names mentioned in this manual are either registered trademarks or trademarks of their respective companies.

In some cases, trademark symbols such as [™] or [®] are not specified in this manual.