



Vulnerabilities of MELSEC-Q Series Ethernet Interface Modules (Identified by External Institutions)

■Date of Issue

June 2019

■Relevant Models

QJ71E71-100

Thank you for your continued support of Mitsubishi Electric programmable controllers, MELSEC-Q series. We will inform you of vulnerabilities of MELSEC-Q series Ethernet interface modules (hereinafter referred to as Ethernet module) identified by external institutions, and the measures that must be taken by users.

1 OVERVIEW

Relevant models

QJ71E71-100

Impact

If the Ethernet module is directly connected to the Internet (without a firewall), a third-party may send a TCP packet that FTP login name is intentionally changed to the name with more than 155 characters, resulting in the following problems:

- System error occurrence of Ethernet module and termination of Ethernet communication (Reset the CPU or turn off power to recover Ethernet communication.)

(References) Web site of external institution

Institution that identified the vulnerabilities	Web site
ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)	ics-cert.us-cert.gov/advisories/ICSA-19-141-02
JPCERT (Japan Computer Emergency Response Team)	jvn.jp/vu/JVNVU93268101

2 MEASURES TAKEN BY USERS

As described in the user's manual for Ethernet modules^{*1}, specify the FTP login name with up to 12 characters to operate normally the Ethernet module.

As described in the "WARNING" of [Design Precautions] in the user's manual for Ethernet modules^{*2}, to maintain the safety of the Mitsubishi Electric programmable controller system against unauthorized access from external devices via the Internet, take measures such as installing a firewall. For details, refer to the user's manual for Ethernet modules^{*2}.

*1  MELSEC-Q/L Ethernet Interface Module User's Manual (Application)

*2  Q Corresponding Ethernet Interface Module User's Manual (Basic)

In addition, for whether modules used are affected or not, for instance, whether the modules are connected to the Internet or not, or whether measures such as firewalls are taken or not, please contact your IT department or local supplier.

1. Checking for the Internet connection

Check whether the Ethernet modules installed on any used equipment are connected to the Internet or not.

2. Checking for firewalls

If the Ethernet modules are connected to the Internet, check whether measures such as a firewall are taken in the network systems.

3 MEASURES FOR ETHERNET MODULES

To enhance the security of the Ethernet modules, the following modules are taken measures to keep the Ethernet communication.

Relevant modules

Ethernet modules with a serial number (first five digits) of "20122" or later

REVISIONS

Version	Date of Issue	Revision
A	June 2019	First edition