MITSUBISHI ELECTRIC

TECHNICAL BULLETIN

[Issue No.]	FA-A-0230
[Title]	Vulnerabilities of MELSEC-Q series Ethernet interface modules (identified by external institutions)
[Date of Issue]	December 2016
[Relevant Models]	QJ71E71-100, QJ71E71-B5, QJ71E71-B2

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, QJ71E71-B5, QJ71E71-B2

Impact

If the Ethernet module is directly connected to the Internet (without a firewall), a third-party may analyze communication data or occupy the communication port, resulting in the following problems:

- Unauthorized upload and download of programs and others
- Termination of TCP/IP communications using MELSOFT application

For details, visit the following websites:

Institution that identified the vulnerabilities	Web site
ICS-SERT (Industrial Control Systems Cyber Emergency Response Team)	ics-cert.us-cert.gov/advisories/ICSA-16-336-03
JPCERT (Japan Computer Emergency Response Team)	jvn.jp/vu/JVNVU99901500

2   Measures taken by users

As described in the "WARNING" of [Design Precautions] in the user's manual for the Ethernet modules[1], 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 the Ethernet modules[1].

*1   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.

MITSUBISHI ELECTRIC CORPORATION

3 Additional function

To enhance the security of the Ethernet modules, the IP filter function has been added.

For details, refer to the user's manual for the Ethernet modules[*1].

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

IP filter function

This function improves unauthorized access prevention by identifying IP address of the access source with IP address specification.

Models supporting the IP filter function

Ethernet modules with a serial number (first five digits) of "18072" or later