

## Vulnerabilities of FTP Server Function for MELSEC-Q Series and MELSEC-L Series CPU Modules

**■Date of Issue**

November 2019

**■Relevant Models**

QCPU with built-in Ethernet port, LCPU with built-in Ethernet port

Thank you for your continued support of Mitsubishi Electric programmable controllers, MELSEC-Q series and MELSEC-L series.

We will inform you of vulnerabilities of FTP server function for the MELSEC-Q series and MELSEC-L series CPU modules. Please take measures against the vulnerabilities as described below.

### 1 OVERVIEW

#### Relevant models

Module	Model	First five digits of a serial number
QCPU with built-in Ethernet port	<ul style="list-style-type: none"> <li>• Q03UDVCPU</li> <li>• Q03UDECPU</li> <li>• Q04UD(P)VCPU</li> <li>• Q04UDEHCPU</li> <li>• Q06UD(P)VCPU</li> <li>• Q06UDEHCPU</li> <li>• Q10UDEHCPU</li> <li>• Q13UD(P)VCPU</li> <li>• Q13UDEHCPU</li> <li>• Q20UDEHCPU</li> <li>• Q26UD(P)VCPU</li> <li>• Q26UDEHCPU</li> <li>• Q50UDEHCPU</li> <li>• Q100UDEHCPU</li> </ul>	"21081" or earlier
LCPU with built-in Ethernet port	<ul style="list-style-type: none"> <li>• L02CPU(-P)</li> <li>• L06CPU(-P)</li> <li>• L26CPU(-P)</li> <li>• L26CPU(-P)BT</li> </ul>	"21101" or earlier

FA-A-0290-A

### Impact

MELSEC-Q series and MELSEC-L series CPU modules have the vulnerabilities of FTP server resource depletion (CWE-400). Depending on the timing at which an attacker connects to the FTP server on the relevant models, the FTP service may enter a denial-of-service condition<sup>\*1</sup> and a normal FTP client may not access the FTP server. Only FTP server function is affected by the vulnerabilities.


\*1 The denial-of-service (DoS) condition means the condition that an attacker interferes with the FTP service operations. (Reference) URLs of external institution

External institution	URL
ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)	ics-cert.us-cert.gov/advisories/ICSA-19-311-01
JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)	jvn.jp/vu/JVNVU97094124

## 2 RECOVERY METHODS

If you cannot connect to the FTP server due to this vulnerability, you can recover the connection using any one of the following methods.

- Deactivate the FTP server forcibly on "Status of Each Connection" tab of "Ethernet Diagnostics" window in GX Works2, and then activate the FTP server.

 [Diagnostics] ⇒ [Ethernet Diagnostics]


- Unplug the Ethernet cable from the CPU module, and connect it again after one minute.

## 3 MEASURES TAKEN BY USERS

As described in the "WARNING" of [Design Precautions] in the user's manual for the Ethernet modules<sup>\*1\*2</sup>, take measures such as installing a firewall against unauthorized access from external devices via the Internet. For whether your modules are connected to the Internet or not, and for whether measures such as firewalls are taken or not, please contact your IT department or local supplier.

Item	Description
Internet	Check whether the CPU modules installed on any used modules are connected to the Internet or not.
Measures	If the Ethernet modules are connected to the Internet, check whether measures such as a firewall are taken in the network systems.

\*1  QnUCPU User's Manual (Communication via Built-in Ethernet Port)

\*2  MELSEC-L CPU Module User's Manual (Built-In Ethernet Function)

## 4 MEASURES FOR CPU MODULES

To enhance security, the CPU module automatically disconnects to the FTP client when the module does not receive the operation instructions from the FTP client during a fixed time.

- Modules supporting the function

Module	First five digits of a serial number
MELSEC-Q series CPU module	"21082" or later
MELSEC-L series CPU module	"21102" or later

FA-A-0290-A

---

**REVISIONS**

Version	Date of Issue	Revision
A	November 2019	First edition