Vulnerability of FTP server function on MELSEC Q/L Series CPU modules

November 7th, 2019
Mitsubishi Electric Corporation

■Overview

A vulnerability was found in FTP server function on MELSEC-Q Series CPUs with serial number (first 5 digits) 21081 or before and MELSEC-L Series CPUs with serial number (first 5 digits) 21101 or before. The FTP service on the attacked module might enter a DoS condition(*1) when an attacker connects to it by exploiting this vulnerability. The versions of the MELSEC-Q and MELSEC-L Series CPUs affected by this vulnerability are listed as follows. In the case of using the affected products, take defensive measures described in the mitigations to minimize the risk of exploitation of this vulnerability.

*1 DoS (Denial-of-Service) condition refers to the state where the service is blocked by an attacker.

■Affected products

Affected products are as follows.

<MELSEC-Q Series>
Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU : First 5 digits of serial number is 21081 or before,
Q03/04/06/13/26UDVCPU : First 5 digits of serial number is 21081 or before,
Q04/06/13/26UDPVCPU : First 5 digits of serial number is 21081 or before.

<MELSEC-L Series>
L02/06/26CPU, L26CPU-BT : First 5 digits of serial number is 21101 or before,
L02/06/26CPU-P, L26CPU-PBT : First 5 digits of serial number is 21101 or before,
L02/06/26CPU-CM, L26CPU-BT-CM : First 5 digits of serial number is 21101 or before.

The serial number of CPU module can be checked on the rating plate on the side of the module, or checked in "System monitor" of GX Works2.

■Description

The FTP server function on MELSEC-Q Series CPU modules and MELSEC-L Series CPU modules has a vulnerability, CVE-2019-13555, of Uncontrolled Resource Consumption (CWE-400).

■Impact

A remote attacker can cause the FTP service to enter a DoS condition dependent on the timing at which a remote attacker connects to the FTP server on the above CPU modules and the authorized FTP clients will not be able to connect to the FTP server. Only the FTP server function is affected by this vulnerability.

■How to recover

You can recover the FTP server by either of the following methods.

(1) Deactivate the FTP server from "Status of Each Connection" of "Ethernet Diagnostics" on GX Works2, and then activate the FTP server again.
(2) Disconnect the Ethernet cable from the CPU module, and reconnect it after 1 minute.

■Measures for CPU modules

We have started manufacturing the following CPU modules to automatically disconnect FTP connection if there is no operation from FTP client for a certain period of time in order to improve security.

<MELSEC-Q Series>
First 5 digits of serial number is 21082 or later.

<MELSEC-L Series >
First 5 digits of serial number is 21102 or later.

■Mitigations

As described at the ″WARNING″ of [Design Precautions] in the user's manual for CPU modules (*2), to maintain the security of the Mitsubishi Electric programmable controller system against unauthorized access from external devices via the Internet, please take measures such as installing a firewall. For details, refer to the user's manual for CPU modules

*2 QnUCPU User's Manual(Communication via Built-in Ethernet Port) and MELSEC-L CPU Module User's Manual (Built-in Ethernet Function)

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

1. Checking for the Internet connection

Please check whether the CPU modules used are connected to the Internet or not.

2. Checking for firewalls

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

■Acknowledgement

Mitsubishi Electric thanks Tri Quach of Amazon's Customer Fulfillment Technology Security (CFTS) group who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.