Remote Access Vulnerability in MELSOFT Transmission Port (UDP/IP)

March 30, 2020
Mitsubishi Electric Corporation

■Overview

Mitsubishi Electric is aware of a vulnerability of Uncontrolled Resource Consumption (CWE-400) in MELSOFT transmission port (UDP/IP) of MELSEC iQ-R, iQ-F, Q, L and F series programmable controllers. When an attacker sends a large amount of data to the MELSOFT transmission port (UDP/IP) of the applicable product, the MELSOFT transmission port (UDP/IP) may enter an unprocessable condition.

■Affected products

All versions of MELSEC iQ-R, iQ-F, Q, L and F series programmable controllers with MELSOFT transmission port (UDP/IP) in Ethernet port are affected.

■Description

There is a vulnerability of Uncontrolled Resource Consumption (CWE-400) in MELSOFT transmission port (UDP/IP) of MELSEC iQ-R, iQ-F, Q, L and F series programmable controllers provided by Mitsubishi Electric Corporation.

■Impact

When the MELSOFT transmission port enters an unprocessable condition, authorized clients cannot connect to the MELSOFT transmission port, and devices communicating on other transmission ports are difficult to connect. In addition, this vulnerability will not affect functions other than Ethernet communication.

■Mitigations

For unauthorized access from external devices via the Internet, as a warning described in [Design Precautions] given in user's manuals*1, when it is necessary to maintain the safety of the programmable controller system, take measures such as installing a firewall.

*1 E.g. MELSEC iQ-R Ethernet User's Manual (Application)

Moreover, damage caused by this vulnerability can be mitigated or prevented by implementing either or a combination of the following methods.

(1) Install a firewall.

(2) Use the IP filter function to restrict the connectable IP addresses.

■Acknowledgements

Mitsubishi Electric would like to thank Rongkuan Ma, Jie Meng and Peng Cheng who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.