Denial-of-Service Vulnerability in MELSEC iQ-R Series Ethernet Port

■Overview

Mitsubishi Electric is aware of a denial-of-service (DoS) vulnerability in MELSEC iQ-R series modules due to uncontrolled resource consumption. When the CPU module receives a specially crafted packet from a malicious attacker, program execution and communication may enter a DoS condition. (CVE-2020-16850)
The product models and firmware versions affected by this vulnerability are listed below.

■Affected products

The following MELSEC iQ-R series modules are affected:
・R00/01/02CPU：all versions
・R04/08/16/32/120(EN)CPU：all versions
・R08/16/32/120SFCPU：all versions
・R08/16/32/120PCPU：all versions
・R16/32/64MTCPU：all versions

■Description

A denial-of-service (DoS) vulnerability due to uncontrolled resource consumption (CWE-400) exists in MELSEC iQ-R series modules.

■Impact

When the CPU module receives a specially crafted packet from a malicious attacker, program execution and communication may enter a DoS condition, and a reset is required to recover it.

■Countermeasures

The fixed version of the firmware is going to be released soon.

■Mitigations

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:
- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.

■Acknowledgement

Mitsubishi Electric would like to thank Yossi Reuven of SCADAfence Ltd. who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.