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

Release date: October 8, 2020
Last update date: May 18, 2021
Mitsubishi Electric Corporation

■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, an error may occur on the CPU module and then the 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: Firmware versions "20" and earlier
- R04/08/16/32/120(EN)CPU: Firmware versions "52" and earlier
- R08/16/32/120SFCPU: Firmware versions "22" and earlier
- R08/16/32/120PCPU: Firmware versions "25" and earlier
- R08/16/32/120PSFCPU: Firmware versions "06" and earlier
- R16/32/64MTCPU: Firmware versions "21" and earlier

■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, an error may occur on the CPU module and then the program execution and communication may enter a DoS condition, and a reset is required to recover it.

■Countermeasures

The following modules have been fixed.

- R00/01/02CPU: Firmware versions "21" or later
- R04/08/16/32/120CPU, R04/08/16/32/120ENCPU: Firmware versions "53" or later
- R08/16/32/120SFCPU: Firmware versions "23" or later
- R08/16/32/120PCPU: Firmware versions "26" or later
- R08/16/32/120PSFCPU: Firmware versions "07" or later
- R16/32/64MTCPU: Firmware versions "22" or later

■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.

< Inquiries | MITSUBISHI ELECTRIC FA >

https://www.mitsubishielectric.com/fa/support/index.html

■Update history

May 18, 2021

Added affected product(R08/16/32/120PSFCPU). Added R16/32/64MTCPU that has been fixed to “Countermeasures”.

February 18, 2021

Added modules that have been fixed to “Countermeasures”.

October 26, 2020

Added modules that have been fixed to “Countermeasures”.