Denial-of-Service Vulnerability in MELSEC iQ-R Series C Controller Module

Release date: October 7, 2021
Mitsubishi Electric Corporation

■Overview

Denial-of-Service (DoS) vulnerability exists in MELSEC iQ-R series C Controller Module due to uncontrolled resource consumption (CWE-400). A remote attacker could prevent the module from starting up by sending a large number of packets to the module starting up in a short time (CVE-2021-20600).

The product models and firmware versions affected by this vulnerability are listed below.

■CVSS

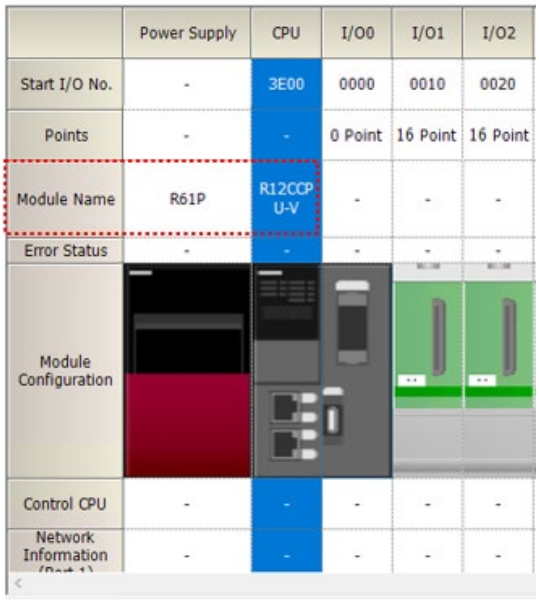
CVE-2021-20600 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H Base Score: 6.8

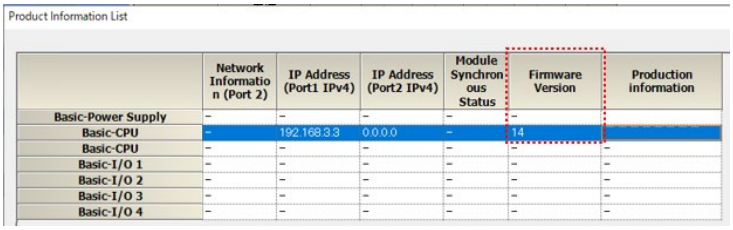
■Affected products

The following modules are affected:

Module Name	Firmware Version
R12CCPU-V	all versions

The Module Name and Firmware Version of the module can be checked on the window of system monitor in CW Configurator.





■Description

Denial-of-Service (DoS) vulnerability due to uncontrolled resource consumption (CWE-400) exists in MELSEC iQ-R series C Controller Module.

■Impact

A System WDT error occur and the module may not start if remote attacker sends a large number of packets in a short time while the C Controller Module starting up *1. However, this problem occurs only when a large number of packets are received in a short time during startup, and does not occur after startup normally.

*1 Starting means that the READY LED is blinking. After startup normally, the READY LED will light up.

■Countermeasures

Countermeasures are under consideration. Please implement Mitigations/Workarounds.

■Mitigations/Workarounds

There is a possibility that C Controller Module has been attacked by exploiting this vulnerability if a System WDT error occurs while the the module starting up. In this case, please disconnect the LAN cable of the module and start it. After confirming that the module has started normally, make a LAN connection.

In addition, regardless of whether or not the above error occurred, 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.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

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