Denial-of-Service Vulnerability in Ethernet Port on CPU Module of MELSEC iQ-F Series

Release date: December 10, 2020
Mitsubishi Electric Corporation

■Overview

Mitsubishi Electric is aware of a denial-of-service (DoS) vulnerability in MELSEC iQ-F series FX5U(C) CPU modules. CPU modules allow malicious attacker to cause a DoS condition on program execution and communication by sending specially crafted ARP packets. (CVE-2020-5665)

■CVSS

CVE-2020-5665: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H Base Score: 7.4

■Affected products

The following products are affected.

・FX5U(C) CPU module: firmware version 1.060 or earlier

The firmware version of the module can be checked on System Monitor(Fig 1) in GX Works3.

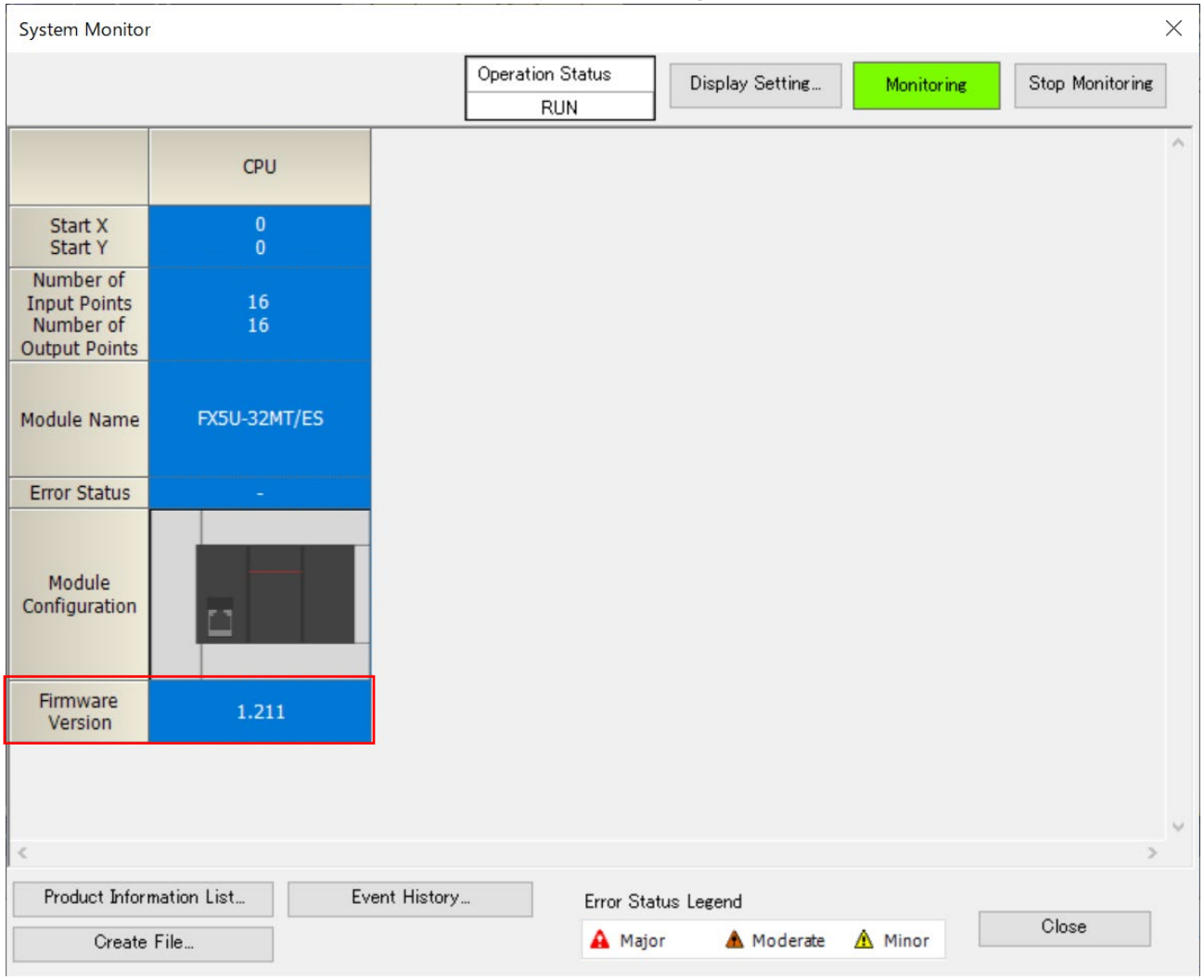

Fig 1 System Monitor

■Description

A denial-of-service (DoS) vulnerability due to improper check or handling of exceptional conditions (CWE-703) exists in MELSEC iQ-F series modules.

■Impact

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

■Countermeasures

Please download version 1.061 or later from the following site and update the firmware. For how to update firmware,please refer to “JY997D55401_MELSEC iQ-F FX5 User’s Manual (Application)”.

https://www.mitsubishielectric.com/fa/#software

■Mitigations

Mitsubishi Electric recommends that our 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 the LAN and ensure that they are not accessible from untrusted networks and hosts.

■Contact information

Please contact your local Mitsubishi Electric representative.