Denial of Service (DoS) Vulnerability
in MELSEC-F Series Ethernet interface block

Release date: January 13, 2022
Mitsubishi Electric Corporation

■Overview
Denial of Service (DoS) vulnerability exists in a Ethernet interface block of MELSEC-F series. A malicious attacker may cause DoS condition in communication function of the product by sending specially crafted packets. (CVE-2021-20613)
The product models and firmware versions affected by this vulnerability are listed below.

■CVSS
CVE-2021-20613 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

■Affected products
The following products and versions are affected:

- FX3U-ENET:Firmware version 1.16 and prior
- FX3U-ENET-L:Firmware version 1.16 and prior
- FX3U-ENET-P502:Firmware version 1.16 and prior

The product version is indicated by "VERSION" on the label attached to the right side of the product.

■Description
Denial of Service (DoS) vulnerability exists in the Ethernet interface block of MELSEC-F series due to Improper Initialization (CWE-665)

■Impact
A malicious attacker may cause DoS condition in communication function of the product(*) by sending specially crafted packets.
In addition, system reset is required for recovery.
* Control by MELSEC-F series PLC is not affected.

■Countermeasures
The fixed products and versions are as follows:

- FX3U-ENET:Firmware version 1.17 or later
- FX3U-ENET-L:Firmware version 1.17 or later
- FX3U-ENET-P502:Firmware version 1.17 or later

■Workarounds
In order to minimize the risk of exploiting this vulnerability, Mitsubishi Electric recommends customers to take the following mitigation.

- 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