Denial-of-Service (DoS) Vulnerability due to OpenSSL Vulnerability in MELSEC iQ-F OPC UA Unit

Release date: October 01, 2024
Mitsubishi Electric Corporation

Overview

Denial-of-Service (DoS) vulnerability due to OpenSSL vulnerability exists in MELSEC iQ-F OPC UA Unit. A malicious remote attacker could cause denial-of service (DoS) condition on the product by getting a legitimate user to import a specially crafted PKCS#12 format certificate. (CVE-2024-0727)

CVSS[1]

CVE-2024-0727 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

Affected products and firmware versions are below.

Series	Model Name	Affected firmware version
MELSEC iQ-F Series	FX5-OPC	All versions

Description

A Denial-of-Service (DoS) vulnerability (CVE-2024-0727) due to NULL Pointer Dereference (CWE-476[2]) when processing PKCS#12[Note 1] format certificate exists in OpenSSL installed on MELSEC iQ-F OPC UA Unit. Because OpenSSL does not correctly check if a certain field in the PKCS#12 format certificate is NULL, a NULL pointer dereference occurs when the field is NULL, causing the product to enter a denial-of-service (DoS) condition.

[Note 1] A file format for storing both private key and X.509 certificate.

Impact

A malicious remote attacker could cause denial-of service (DoS) condition on the product by getting a legitimate user to import a pecially crafted PKCS#12 format certificate. A reset of the product is required for recovery.

Countermeasures for Customers

There are no plans to release a fixed version. Please carry out Mitigations.

Mitigations

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting this vulnerability:

- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Restrict physical access to the product, as well as to computers and network devices located within the same network as the product.
- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use IP filter function to block access from untrusted hosts. For details on the IP filter function, please refer to the following manual.
  MELSEC iQ-F FX5 OPC UA Module User's Manual "4.4 IP Filter"
- Do not import untrusted certificates.

Contact information

Please contact your local Mitsubishi Electric representative.
< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/476.html