Multiple Vulnerabilities due to OpenSSL Vulnerabilities in multiple FA products

Release date: December 21, 2023
Mitsubishi Electric Corporation

Overview

Multiple vulnerabilities due to OpenSSL vulnerabilities exist in multiple Mitsubishi Electric FA products. An attacker could disclose information in the product or could cause Denial-of-Service (DoS) condition. (CVE-2022-4304, CVE-2022-4450, CVE-2023-0286)

CVSS[1]

CVE-2022-4304	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	Base Score: 5.9
CVE-2022-4450	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score: 7.5
CVE-2023-0286	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H	Base Score: 7.4

Affected products

The affected products and versions are as follows.

Products	Module Name	Versions	Applicable Vulnerability
GT SoftGOT2000	-	1.275M to 1.290C	CVE-2023-0286
OPC UA data collector	SW1DND-DCOPCUA-M SW1DND-DCOPCUA-MD	1.04E and prior	CVE-2023-0286
MX OPC Server UA (Software packaged with MC Works64)	SW4DND-MCWDV-MT, etc.	3.05F and later (Packaged with MC Works64 Version 4.03D and later.)	CVE-2022-4304
OPC UA server unit	RD81OPC96	All versions	CVE-2022-4304
FX5-OPC	FX5-OPC	1.006 and prior	CVE-2022-4304 CVE-2022-4450

Description

The following three vulnerabilities exist in multiple FA products.

CVE ID	Vulnerability description
CVE-2022-4304	An information disclosure vulnerability due to Observable Timing Discrepancy (CWE-208[2]) in RSA decryption implementations.
CVE-2022-4450	A Denial-of-Service (DoS) vulnerability due to Double Free (CWE-415[3]) when reading a PEM file.
CVE-2023-0286	An information disclosure and Denial-of-Service (DoS) vulnerability due to Access of Resource Using Incompatible Type ('Type Confusion') (CWE-843[4]) relating to X.400 address processing inside an X.509 GeneralName.

Impact

An attacker could disclose information in the product or could cause Denial-of-Service (DoS) condition.

CVE-2022-4304: By sending specially crafted packets and performing a Bleichenbacher style attack (*1), an attacker could decrypt the ciphertext and disclose sensitive information.
*1: An attack method to decrypt ciphertext by observing the behavior when a padding error occurs.
CVE-2022-4450: An attacker could cause denial-of-service (DoS) on the product by leading a legitimate user to importing a malicious certificate.
CVE-2023-0286: An attacker could disclose sensitive information in memory of the product or cause denial-of-service (DoS) on the product by getting to load a specially crafted Certificate Revocation List (CRL).

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/208.html
3 https://cwe.mitre.org/data/definitions/415.html
4 https://cwe.mitre.org/data/definitions/843.html

Countermeasures

Please take the following countermeasures.

Products	Countermeasures
GT SoftGOT2000	Update the product to version 1.295H or later.
OPC UA data collector	Update the product to version 1.05F or later.
MX OPC Server UA (Software packaged with MC Works64)	Carry out mitigations/workarounds.
OPC UA server unit	Carry out mitigations/workarounds.
FX5-OPC	Update the product to version 1.010 or later.

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities:

1. GT SoftGOT2000 and OPC UA data collector
   - Do not load untrusted Certificate Revocation Lists (CRLs).

2.MX OPC Server UA
   - 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.

3. OPC UA server unit
   - 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.
   - Set a security policy other than 'None' in Security setting function to prevent unauthorized access. For details on Security setting function , please refer to the following manual.
     MELSEC iQ-R OPC UA Server Unit User's Manual (Application) "1.1 OPC UA Server Function"

4. FX5-OPC
Mitigations for CVE-2022-4304
   - 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 the 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"

Mitigations for CVE-2022-4450
   - 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