複数の FA 製品における OpenSSL に起因する 情報漏えい及びサービス拒否(DoS)の脆弱性

公開日 2023 年 12 月 21 日
三菱電機株式会社

■概要

三菱電機製の複数の FA 製品において、OpenSSL に起因する複数の脆弱性が存在することが判明しました。これらの脆弱性を攻撃者に悪用された場合に、当該製品の情報の漏えいが発生したり、当該製品がサービス停止(DoS)状態に陥ったりする可能性があります。(CVE-2022-4304、CVE-2022-4450、CVE-2023-0286)

■CVSS スコア [1]

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

■該当製品と影響を受ける脆弱性

影響を受ける製品は、以下の通りです。

製品名	形名	バージョン	該当する脆弱性
GT SoftGOT2000	-	1.275M ～ 1.290C	CVE-2023-0286
OPC UA データコレクタ	SW1DND-DCOPCUA-M SW1DND-DCOPCUA-MD	1.04E 以前	CVE-2023-0286
MX OPC Server UA (MC Works64 同梱ソフトウェア)	SW4DND-MCWDV-MT 他	3.05F 以降 (MC Works64 Version4.03D 以降に同梱)	CVE-2022-4304
OPC UA サーバユニット	RD81OPC96	全バージョン	CVE-2022-4304
FX5-OPC	FX5-OPC	1.006 以前	CVE-2022-4304 CVE-2022-4450

■脆弱性の説明

複数の FA 製品には、以下の 3 件の脆弱性が存在します。

CVE ID	脆弱性の説明
CVE-2022-4304	RSA での復号の実装に存在するタイミングの違いに起因する情報漏えい(CWE-208[2])による、情報漏えいの脆弱性
CVE-2022-4450	PEM 形式のデータの読み込み時の二重解放(CWE-415[3])による、サービス拒否(DoS)の脆弱性
CVE-2023-0286	X.509 GeneralName 内の X.400 アドレス処理に存在する型の取り違え(CWE-843[4])による、情報漏えい及びサービス拒否(DoS)の脆弱性

■脆弱性がもたらす脅威

これらの脆弱性を攻撃者に悪用された場合、当該製品の情報の漏えいが発生したり、当該製品がサービス停止(DoS)状態に陥ったりする可能性があります。

CVE-2022-4304　攻撃者は、細工したパケットを送信し、Bleichenbacher 攻撃(*1)を行うことにより、暗号文を解読し、機微な情報を窃取できる可能性があります。
*1:パディングエラーが発生した際の実行時間の違いを観察することにより、暗号文の解読を行う攻撃

CVE-2022-4450　攻撃者は、悪意のある証明書をインポートすることにより、当該製品をサービス停止(DoS)状態に陥らせることができる可能性があります。

CVE-2023-0286　攻撃者は、当該製品に細工した証明書失効リスト(CRL)を読み込ませることにより、メモリ内の機微な情報を窃取したり、当該製品をサービス停止(DoS)状態に陥らせることができる可能性があります。

[1] https://www.ipa.go.jp/security/vuln/CVSSv3.html
[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

■対策方法

下記の対応をお願いいたします。

製品	対策方法
GT SoftGOT2000	当該製品を 1.295H 以降へバージョンアップしてください。
OPC UA データコレクタ	当該製品を 1.05F 以降へバージョンアップしてください。
MX OPC Server UA (MC Works64 同梱ソフトウェア)	軽減策・回避策で対応ください。
OPC UA サーバユニット	軽減策・回避策で対応ください。
FX5-OPC	当該製品を 1.010 以降へバージョンアップしてください。

■軽減策・回避策

本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。

1. GT SoftGOT2000 及び OPC UA データコレクタ

・信頼できない証明書失効リスト(CRL)を読み込まないでください。

2. MX OPC Server UA

・当該製品を LAN 内で使用し、信頼できないネットワークやホストからのアクセスをファイアウォールでブロックしてください。
・当該製品、当該製品と同一のネットワーク内に配置されたパソコンおよびネットワーク機器への物理的なアクセスを制限してください。
・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止してください。

3. OPC UA サーバユニット

・当該製品を LAN 内で使用し、信頼できないネットワークやホストからのアクセスをファイアウォールでブロックしてください。
・当該製品、当該製品と同一のネットワーク内に配置されたパソコンおよびネットワーク機器への物理的なアクセスを制限してください。
・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止してください。
・当該製品のセキュリティ設定機能にて、None 以外のセキュリティポリシーを設定し、不正アクセスを防止してください。
セキュリティ設定機能については、以下のマニュアルを参照ください。
「MELSEC iQ-R OPC UA サーバユニット ユーザーズマニュアル(応用編)」の「1.1 OPC UA サーバ機能」

4. FX5-OPC

CVE-2022-4304 に対する軽減策
・当該製品を LAN 内で使用し、信頼できないネットワークやホストからのアクセスをファイアウォールでブロックしてください。
・当該製品、当該製品と同一のネットワーク内に配置されたパソコンおよびネットワーク機器への物理的なアクセスを制限してください。
・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止してください。
・当該製品の IP フィルタ機能を使用し、信頼できないホストからのアクセスをブロックしてください。
IP フィルタ機能については、以下のマニュアルを参照ください。
「MELSEC iQ-F FX5 OPC UA ユニットユーザーズマニュアル」の「4.4 IP フィルタ」
CVE-2022-4450 に対する軽減策
・信頼できない証明書をインポートしないでください。

■お客様からのお問い合わせ先

製品をご購入いただいた当社の支社、代理店にご相談ください。

〈お問い合わせ | 三菱電機 FA〉
https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html