MELSEC iQ-F OPC UA ユニットにおける OpenSSL に起因するサービス拒否(DoS)の脆弱性

公開日 2024 年 10 月 1 日
三菱電機株式会社

■概要

MELSEC iQ-F OPC UA ユニットに搭載している OpenSSL において、サービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、悪意のある PKCS#12 形式の証明書ファイルを当該製品にインポートさせることより、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。

■CVSS スコア [1]

CVE-2024-0727　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H　基本値:7.5

■該当製品の確認方法

影響を受ける製品は、以下の通りです。

シリーズ	製品形名	バージョン
MELSEC iQ-F シリーズ	FX5-OPC	全バージョン

■脆弱性の説明

MELSEC iQ-F OPC UA ユニットに搭載している OpenSSL には、PKCS#12[注 1]形式の証明書ファイルを処理する際の NULL ポインタ参照(CWE-476[2])に起因するサービス拒否(DoS)の脆弱性が存在します。OpenSSL が、PKCS#12 形式の証明書ファイルの特定のフィールドが NULL であることを正しくチェックしないため、特定のフィールドが NULL である場合に、NULL ポインタ参照が発生し、当該製品がサービス停止(DoS)状態に陥ります。

[注 1]秘密鍵とそれに関連付けられた X.509 証明書を保存するために使用されるファイル形式です。

■脆弱性がもたらす脅威

攻撃者は、悪意のある PKCS#12 形式の証明書ファイルを当該製品にインポートさせることより、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。なお、復旧には当該ユニットのリセットが必要です。

■お客様での対応

対策版のリリース予定はございませんので、該当製品をご使用のお客様は、下記の軽減策にて対応をお願いいたします。

■軽減策

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。

・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 ユーザーズマニュアル(OPC UA 編)「4.4 IP フィルタ」
・信用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

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/476.html