複数の FA 製品の Ethernet 機能におけるサービス拒否(DoS)の脆弱性

公開日 2024 年 2 月 27 日
三菱電機株式会社

■概要

複数の FA 製品の Ethernet 機能において、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、当該製品に対して TCP SYN Flood 攻撃※1 を行うことにより、当該製品の Ethernet 通信を一定時間サービス停止(DoS)状態に陥らせることができる可能性があります。(CVE-2023-7033)

※1:DoS 攻撃の手法の一つで、TCP の接続要求を行う SYN パケットのみを大量に送りつける攻撃です。

■CVSS スコア [1]

CVE-2023-7033 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L 基本値 5.3

■該当製品の確認方法

影響を受ける製品とバージョンは以下の通りです。

シリーズ	製品形名	バージョン
MELSEC iQ-F シリーズ	FX5U-xMy/z x=32, 64, 80, y=T, R, z=ES, DS, ESS, DSS	全バージョン
	FX5UC-xMy/z x=32, 64, 96, y=T, z=D, DSS	全バージョン
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	全バージョン
	FX5UJ-xMy/z x=24, 40, 60, y=T, R, z=ES, DS, ESS, DSS	全バージョン
	FX5S-xMy/z x=30, 40, 60, y=T, R, z=ES, ESS	全バージョン

■脆弱性の説明

複数の FA 製品の Ethernet 機能には、不十分なリソースプール(CWE-410[2])に起因するサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は、当該製品に対して TCP SYN Flood 攻撃を行うことにより、当該製品の Ethernet 通信を一定時間サービス停止(DoS)状態に陥らせることができる可能性があります。

■対策方法

軽減策・回避策にて対応をお願いいたします。

■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。

・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。
・IP フィルタ機能※2 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。
・当該製品および当該製品が接続された LAN への物理的なアクセスを制限してください。

※2: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(通信編)「13.1 IP フィルタ機能」

■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/410.html