MELSEC F シリーズ Ethernet インタフェースブロックにおける サービス拒否（DoS）及び潜在的な不特定の脆弱性

公開日 2022 年 1 月 13 日
三菱電機株式会社

■概要

MELSEC F シリーズ Ethernet インタフェースブロックに、サービス拒否（DoS）及び潜在的な不特定の脆弱性が存在することが判明しました。悪意のある攻撃者からの不正なパケットを受信すると、該当製品の通信機能が DoS 状態に陥ったり、その他不特定の影響を受ける可能性があります。（CVE-2021-20612）

この脆弱性の影響を受ける製品形名およびバージョンを以下に示します。

■CVSS スコア

CVE-2021-20612 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

影響を受ける製品及びバージョンは以下の通りです。

・FX3U-ENET：ファームウェアバージョン 1.14 以前
・FX3U-ENET-L：ファームウェアバージョン 1.14 以前
・FX3U-ENET-P502：ファームウェアバージョン 1.14 以前

本製品のバージョンは、製品本体の側面に張り付けられているネームプレートの"VERSION"に記載した番号で確認することができます。

■脆弱性の説明

MELSEC F シリーズ Ethernet インタフェースブロックには、セキュリティに関する管理機能の欠落(CWE-671)により、不要な TCP ポートがオープンしており、サービス拒否(DoS)及び潜在的な不特定の脆弱性が存在します。

■脆弱性がもたらす脅威

不必要にオープンしているポートにおいて、悪意のある攻撃者からの不正なパケットを受信すると、該当製品でエラーが発生して通信機能が DoS 状態に陥ったり(※)、その他不特定の影響を受ける可能性があります。なお、通信機能の DoS 状態からの復旧にはシステムのリセットが必要になります。
※MELSEC F シリーズ 基本ユニットの制御への影響はありません。

■対策方法

修正済み製品及びバージョンは以下の通りです。

・FX3U-ENET：ファームウェアバージョン 1.16 以降
・FX3U-ENET-L：ファームウェアバージョン 1.16 以降
・FX3U-ENET-P502：ファームウェアバージョン 1.16 以降

■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。

・該当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。
・該当製品を 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。

■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