

# 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) の脆弱性

公開日 2021 年 7 月 20 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は、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。悪意のある攻撃者から不正なパケットを受信すると、該当製品による通信が DoS 状態に陥る可能性があります。(CVE-2021-20596) 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-2021-20596 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”に記載した番号で知ることができます。

## ■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、NULL ポインタ参照(CWE-476)により、通信がサービス拒否 (DoS) 状態に陥る脆弱性が存在します。

## ■脆弱性がもたらす脅威

攻撃者から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、通信が DoS 状態に陥る可能性があります。なお、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に影響はありません。

## ■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>