

MELSEC iQ-F シリーズ CPU ユニットの Ethernet ポートにおけるサービス拒否 (DoS) の脆弱性

公開日 2020 年 12 月 10 日
三菱電機株式会社

■概要

MELSEC iQ-F シリーズ FX5U(C)CPU ユニットには、サービス拒否 (DoS) 状態に陥る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 ARP パケットを受信すると、CPU ユニットでエラーが発生し、プログラム実行及び通信が DoS 状態に陥る可能性があります。(CVE-2020-5665)

■CVSS スコア

CVE-2020-5665: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H 基本値: 7.4

■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。

・FX5U(C)CPU ユニット: ファームウェアバージョン 1.060 以前

FX5U(C)CPU ユニットのバージョンは、GX Works3 のシステムモニタ(図 1)で確認することができます。



図 1 システムモニタ

■脆弱性の説明

MELSEC iQ-F シリーズ FX5U(C)CPU ユニットには、例外条件の確認や処理が不適切なため(CWE-703)、プログラム実行及び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 ARP パケットを受信すると、CPU ユニットでエラーが発生し、プログラム実行及び通信が DoS 状態に陥る可能性があります。なお、復旧には CPU ユニットのリセットが必要になります。

■対策方法

以下サイトよりファームウェアバージョン 1.061 以降のファームウェアアップデート情報ファイルをダウンロードしたうえで、アップデートください。アップデート方法につきましては、「JY997D54301 MELSEC iQ-F FX5 ユーザーズマニュアル(応用編)」をご参

照いただきますよう、よろしくお願い致します。

<https://www.mitsubishielectric.co.jp/fa/download/index.html>

■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。
- ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにしてください。

■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>