MELSEC iQ-R シリーズの Ethernet ポートにおける サービス拒否(DoS)の脆弱性

公開日 2020 年 10 月 8 日
最終更新日 2021 年 5 月 18 日
三菱電機株式会社

■概要

MELSEC iQ-R シリーズのユニットには、リソース枯渇によるサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者から不正なパケットを受信すると、CPU ユニットでエラーが発生し、プログラム実行および通信が DoS 状態に陥る可能性があります。(CVE-2020-16850)

この脆弱性の影響を受ける製品形名およびファームウェアバージョンを以下に示します。

■該当製品の確認方法

MELSEC iQ-R シリーズのユニットのうち、次の製品形名とファームウェアバージョンのものが影響を受けます。

・R00/01/02CPU:ファームウェアバージョン"20"以前
・R04/08/16/32/120(EN)CPU:ファームウェアバージョン"52"以前
・R08/16/32/120SFCPU:ファームウェアバージョン"22"以前
・R08/16/32/120PCPU:ファームウェアバージョン"25"以前
・R08/16/32/120PSFCPU:ファームウェアバージョン"06"以前
・R16/32/64MTCPU:ファームウェアバージョン"21"以前

■脆弱性の説明

MELSEC iQ-R シリーズのユニットには、リソース枯渇(CWE-400)によるサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者から不正なパケットを受信すると、CPU ユニットでエラーが発生し、プログラム実行および通信が DoS 状態に陥ります。なお、復旧にはリセットが必要になります。

■対策方法

下記ユニットにおいては、対策を実施済みです。

・R00/01/02CPU:ファームウェアバージョン"21"以降
・R04/08/16/32/120CPU、R04/08/16/32/120ENCPU:ファームウェアバージョン"53"以降
・R08/16/32/120SFCPU:ファームウェアバージョン"23"以降
・R08/16/32/120PCPU:ファームウェアバージョン"26"以降
・R08/16/32/120PSFCPU:ファームウェアバージョン"07"以降
・R16/32/64MTCPU:ファームウェアバージョン"22"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。

・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。

■謝辞

この問題をご報告いただいた SCADAfence Ltd 社 Yossi Reuven 様に感謝いたします。

■お客様からのお問い合わせ先

お客様からのお問い合わせ先につきましては、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

■更新履歴

2021 年 5 月 18 日
影響を受ける製品に R08/16/32/120PSFCPU を追加しました。
R16/32/64MTCPU の対策方法の情報を追加しました。

2021 年 2 月 18 日
「対策方法」に対応済みの製品を追加しました。

2020 年 10 月 26 日

「対策方法」に対応済みの製品を追加しました。