

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 6 月 9 日
最終更新日 2021 年 4 月 20 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 (CWE-400) 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、Ethernet ポートの通信が DoS 状態に陥る可能性があります。

※ DoS (Denial of Service) 状態とは、攻撃者により当該サービスの運用が妨害される状態です。

■該当製品の確認方法

影響を受ける製品は以下の製品です。

- R00/01/02CPU: ファームウェアバージョン"7"以前
- R04/08/16/32/120CPU、R04/08/16/32/120ENCPU: ファームウェアバージョン"39"以前
- R08/16/32/120SFCPU: ファームウェアバージョン"20"以前
- R08/16/32/120PCPU: ファームウェアバージョン"24"以前
- R08/16/32/120PSFCPU: ファームウェアバージョン"05"以前
- RJ71EN71: ファームウェアバージョン"49"以前

ユニットのファームウェアバージョンは GX Works3 のシステムモニタにある下記、製品情報一覧より確認できます。確認方法の詳細な手順は、以下マニュアルを確認ください。

• MELSEC iQ-R ユニット構成マニュアル 付 1 製造情報・ファームウェアバージョン 確認方法

[製品情報一覧]

製品情報一覧

	ネットワーク情報 (ポート2)	IPアドレス (ポート1 IPv4)	IPアドレス (ポート2 IPv4)	ユニット間同期状態	ファームウェアバージョン	製造情報
基本-電源	-	-	-	-	-	-
基本-CPU	-	192.168.3.39	-	-	49	-
基本-I/O 0	-	-	-	-	-	-
基本-I/O 1	-	-	-	-	-	-
基本-I/O 2	-	-	-	-	-	-
基本-I/O 3	-	-	-	-	-	-
基本-I/O 4	-	-	-	-	-	-

■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 (CVE-2020-13238) 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、Ethernet ポートの通信が DoS 状態に陥る可能性があります。

■製品での対応

下記ユニットにおいては、不正なパケットを受け取った場合、パケットを破棄するよう対応しています。

- R00/01/02CPU: ファームウェアバージョン"8"以降
- R04/08/16/32/120CPU、R04/08/16/32/120ENCPU: ファームウェアバージョン"40"以降
- R08/16/32/120SFCPU: ファームウェアバージョン"21"以降
- R08/16/32/120PCPU: ファームウェアバージョン"25"以降
- R08/16/32/120PSFCPU: ファームウェアバージョン"06"以降
- RJ71EN71: ファームウェアバージョン"50"以降

■お客様での対応

信頼できないネットワークやホストからの DoS 攻撃や不正アクセスなどのサイバー攻撃に対しては、お客様にて以下対策を盛り込む必要があります。

1. 信頼できないネットワークやホストへの接続の有無の確認
ご使用中の装置に装着されているユニットにつきまして、信頼できないネットワークやホストへの接続の有無を確認してください。
2. ファイアウォール対策の確認
信頼できないネットワークやホストへの接続がある場合、ファイアウォールの対策が講じられているか確認してください。

お客様にてご使用中の装置における信頼できないネットワークやホストへの接続の有無、ファイアウォール対策有無につきましては、IT 管理部門や装置納入先などへのご確認をお願いいたします。

■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

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。

■更新履歴

2021 年 4 月 20 日

「概要」および「脆弱性がもたらす脅威」の説明を一部修正しました。

2020 年 11 月 5 日

「製品での対応」に対応済みの製品を追加しました。