

# MELSEC iQ-R シリーズ C 言語コントローラユニットにおけるサービス拒否(DoS)の脆弱性

公開日 2021 年 10 月 7 日  
最終更新日 2022 年 7 月 7 日  
三菱電機株式会社

## ■概要

MELSEC iQ-R シリーズ C 言語コントローラユニットには、リソースの枯渇(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。攻撃者は起動中の C 言語コントローラユニットに対して、短時間で大量の packets を送信することにより、当該ユニットの起動を妨げることができる可能性があります。(CVE-2021-20600)  
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。

## ■CVSS スコア

CVE-2021-20600 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H 基本値:6.8

## ■該当製品の確認方法

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。

形名	ファームウェアバージョン
R12CCPU-V	"16"以前

製品の形名およびファームウェアバージョンは、CW Configurator のシステムモニタからご確認いただけます。

	電源	CPU	I/O0	I/O1	I/O2
先頭I/O No.	-	3E00	0000	0010	0020
点数	-	-	0点	16点	16点
ユニット形名	R61P	R12CCP U-V	-	-	-
エラー状態	-	-	-	-	-
ユニット構成					
管理CPU	-	-	-	-	-
ネットワーク情報 (ポート1)	-	-	-	-	-

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	-	192.168.8.3	0.0.0.0	-	14	-
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 C 言語コントローラユニットには、リソースの枯渇(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

攻撃者によって、C 言語コントローラユニットの起動中(\*)に短時間で大量の packets を送信されると、システム WDT エラーが発生して C 言語コントローラユニットが起動しない可能性があります。なお、復旧にはシステムのリセットが必要になります。ただし、本問題は起動中に短時間で大量の packets を受信した場合にのみ発生する現象であり、正常起動後には発生いたしません。

\*READY LED が点滅中の状態を指します。正常起動後は READY LED が点灯します。

## ■対策方法

下記に記載のバージョンで対策済みです。

形名	ファームウェアバージョン
R12CCPU-V	"17"以降

## ■軽減策・回避策

当該製品にて起動中にシステム WDT エラーが発生する場合は、本脆弱性を悪用した攻撃を受けている可能性がありますので、C 言語コントローラユニットの LAN ケーブルを抜き、起動してください。C 言語コントローラユニットの正常起動を確認後、LAN 接続を行ってください。

また、上記エラーの発生有無に関わらず、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。
- ・当該製品を 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>

■更新履歴

2022 年 7 月 7 日

- ・対策方法の内容を更新しました。

2021 年 10 月 28 日

- ・脆弱性がもたらす脅威の内容を更新しました。