MELSEC-Q/L シリーズ Ethernet インタフェースユニット及び MELSEC iQ-R シリーズ MES インタフェースユニットにおけるサービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性

公開日 2022 年 6 月 2 日
三菱電機株式会社

■概要

MELSEC-Q シリーズ及び L シリーズの Ethernet インタフェースユニットの Web 機能及び MELSEC iQ-R シリーズの MES インタフェースユニットの REST サーバ機能に、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在することが判明しました。攻撃者は、該当製品に対して不正なパケットを送信することにより、当該製品をサービス停止(DoS)状態に陥らせたり、悪意のあるプログラムを実行できる可能性があります。(CVE-2022-25163)

この脆弱性の影響を受ける製品名およびバージョンを以下に示しますので、対策または軽減策・回避策の実施をお願いいたします。

■CVSS スコア

CVE-2022-25163 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:8.1

■該当製品の確認方法

影響を受ける製品の形名、およびバージョンは以下の通りです。

シリーズ	形名	対象機能	バージョン
MELSEC-Q シリーズ	QJ71E71-100	Web 機能	シリアル No.の上 5 桁"24061"以前
MELSEC-L シリーズ	LJ71E71-100	Web 機能	シリアル No.の上 5 桁"24061"以前
MELSEC iQ-R シリーズ	RD81MES96N	REST サーバ機能	ファームウェアバージョン"08"以前

シリアル No.およびファームウェアバージョンの確認方法は、以下のマニュアルを参照ください。

QJ71E71-100:

Q 対応 Ethernet インタフェースユニットユーザーズマニュアル(基本編)の「付 11 シリアル No. と機能バージョンの確認方法」

LJ71E71-100:

MELSEC-L Ethernet インタフェースユニットユーザーズマニュアル(基本編)の「付 10 シリアル No., 機能バージョン, MAC アドレスの確認」

RD81MES96N:

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

■脆弱性の説明

MELSEC-Q シリーズ及び L シリーズの Ethernet インタフェースユニットの Web 機能及び MELSEC iQ-R シリーズの MES インタフェースユニットの REST サーバ機能には、不適切な入力確認(CWE-20)による、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者が不正なパケットを送信することにより、当該製品を DoS 状態に陥らせたり、悪意のあるプログラムを実行できる可能性があります。なお、DoS 状態からの復旧及び悪意のあるプログラムが実行された場合の復旧にはシステムのリセットが必要です。

■対策方法

下記に記載のバージョンで対策済みです。

シリーズ	形名	バージョン
MELSEC-Q シリーズ	QJ71E71-100	シリアル No.の上 5 桁"24062"以降
MELSEC-L シリーズ	LJ71E71-100	シリアル No.の上 5 桁"24062"以降
MELSEC iQ-R シリーズ	RD81MES96N	ファームウェアバージョン"09"以降

■軽減策・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)、Web アプリケーションファイアウォール(WAF)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