

MELSEC iQ-R シリーズ Ethernet インタフェースユニットにおける サービス拒否(DoS)の脆弱性

公開日 2022 年 11 月 29 日
三菱電機株式会社

■概要

MELSEC iQ-R シリーズ Ethernet インタフェースユニットには、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、当該製品がサービス停止(DoS)状態に陥る可能性があります。(CVE-2022-40265) 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¹

CVE-2022-40265 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H 基本値:8.6

■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	バージョン
MELSEC iQ-R シリーズ	RJ71EN71	ファームウェアバージョン"65"以前
	R04/08/16/32/120ENCPU(ネットワーク部)	ネットワーク部ファームウェアバージョン"65"以前

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。

・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」
各種製品マニュアルは以下サイトよりダウンロードが可能です。

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

■脆弱性の説明

MELSEC iQ-R シリーズ Ethernet インタフェースユニットには、不適切な入力確認(CWE-20)²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

攻撃者が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)状態に陥らせることができます。なお、DoS 状態から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 iQ-R シリーズ	RJ71EN71	ファームウェアバージョン"66"以降
	R04/08/16/32/120ENCPU(ネットワーク部)	ネットワーク部ファームウェアバージョン"66"以降

以下のサイトより対策済みのバージョン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、アップデートしてください。

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

ファームウェアアップデートの方法は、以下を参照ください。

・MELSEC iQ-R ユニット構成マニュアル「付 2 ファームウェアアップデート機能」

■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)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。
 - ・IP フィルタ機能^{※1} を使用し、接続可能な IP アドレスを適切に制限してください。
- ※1: MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編)セキュリティの「IP フィルタ」を参照ください。

■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>

¹ <https://www.ipa.go.jp/security/vuln/CVSSv3.html>

² <https://cwe.mitre.org/data/definitions/20.html>