

MELSEC iQ-R 及び iQ-L シリーズ並びに MELIPC 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 2022 年 12 月 22 日
最終更新日 2024 年 9 月 5 日
三菱電機株式会社

■概要

MELSEC iQ-R 及び iQ-L シリーズ CPU ユニット並びに MELIPC シリーズには、リソースの不適切なシャットダウンおよびリリース (CWE-404)¹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、当該ユニットの Ethernet 通信がサービス停止(DoS)状態に陥る可能性があります。(CVE-2022-33324)

■CVSS スコア²

CVE-2022-33324 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値: 7.5

■該当製品の確認方法

影響を受ける製品の形名、バージョンは以下のとおりです。

シリーズ	形名	バージョン
MELSEC iQ-R シリーズ	R00/01/02CPU	ファームウェアバージョン"32"以前
	R04/08/16/32/120(EN)CPU	ファームウェアバージョン"65"以前
	R08/16/32/120SFCPU	ファームウェアバージョン"29"以前
	R08/16/32/120PSFCPU	ファームウェアバージョン"08"以前
	R12CCPU-V	ファームウェアバージョン"17"以前
MELSEC iQ-L シリーズ	L04/08/16/32HCPU ※1	ファームウェアバージョン"05"以前
MELIPC シリーズ	MI5122-VW	ファームウェアバージョン"07"以前

※1 本製品は海外一部地域専用品となります。

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」
- ・MELSEC iQ-L Module Configuration Manual "Appendix 1 Checking Production Information and Firmware Version"
- ・MELIPC MI5000 シリーズ ユーザーズマニュアル(スタートアップ編)「付 17 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> (MELSEC iQ-L シリーズ以外)

<https://www.mitsubishielectric.com/fa/download/index.html> (MELSEC iQ-L シリーズ)

■脆弱性の説明

MELSEC iQ-R 及び iQ-L シリーズ CPU ユニット並びに MELIPC シリーズには、リソースの不適切なシャットダウンおよびリリース (CWE-404)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、Ethernet 通信がサービス停止(DoS)状態に陥る可能性があります。なお、復旧には当該ユニットのリセットが必要になります。

■お客様での対応

〈MELSEC iQ-R シリーズの該当製品をご使用中のお客様〉

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」を参照し、ご使用中の製品がファームウェアアップデート可能なバージョンかどうかをご確認ください。

・ファームウェアアップデートが可能な場合

以下のサイトから、次項に記載の対策済み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」

・ファームウェアアップデートが不可の場合

該当製品・該当バージョンをご使用のお客様は、軽減策・回避策にて対応ください。

次項のとおり対策済み製品をリリースしておりますが、対策版へのアップデートは出来ません。

¹ <https://cwe.mitre.org/data/definitions/404.html>

² <https://www.ipa.go.jp/security/vuln/CVSSv3.html>

〈MELIPC シリーズまたは MELSEC iQ-L シリーズの該当製品をご使用中のお客様〉

該当製品・該当バージョンをご使用のお客様は、軽減策・回避策にて対応ください。

次項のとおり対策済み製品をリリースしておりますが、対策版へのアップデートは出来ません。

■ 製品での対応

下記ユニットにおいて、不正なパケットを受信しても、Ethernet 通信が停止しないよう対策済です。

シリーズ	形名	対策バージョン
MELSEC iQ-R シリーズ	R00/01/02CPU	ファームウェアバージョン"33"以降
	R04/08/16/32/120(EN)CPU	ファームウェアバージョン"66"以降
	R08/16/32/120SFCPU	ファームウェアバージョン"30"以降
	R08/16/32/120PSFCPU	ファームウェアバージョン"09"以降
	R12CCPU-V	ファームウェアバージョン"18"以降
MELSEC iQ-L シリーズ	L04/08/16/32HCPU	ファームウェアバージョン"06"以降
MELIPC シリーズ	MI5122-VW	ファームウェアバージョン"08"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)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^{※2}を使用し、信頼できないホストからのアクセスをブロックしてください。

※2: IP フィルタ機能については、以下の各製品のマニュアルを参照ください。

MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編)の 1.13 セキュリティの「IP フィルタ」

MELSEC iQ-L CPU module User's Manual (Application) 24.1 "IP filter Function"

MELSEC iQ-R C 言語コントローラユニット ユーザーズマニュアル(応用編)の 6.6 セキュリティ機能の「IP フィルタ機能」

MELIPC MI5000 シリーズ ユーザーズマニュアル(応用編)の「11.3 IP フィルタ機能」

■ 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

2024 年 9 月 5 日

「該当製品の確認方法」、「製品での対応」に製品を追加しました。

R08/16/32/120PSFCPU、L04/08/16/32HCPU

上記に伴い、タイトルをはじめ全体的に MELSEC iQ-L シリーズの情報を追加しました。

2024 年 7 月 4 日

「お客様での対応」における MELSEC iQ-R シリーズに関する内容を更新しました。

2024 年 5 月 30 日

対策方法に関する内容を更新しました。

「製品での対応」に対策済みの製品を追加しました。

MI5122-VW

2023 年 12 月 12 日

「対策方法」に対策済みの製品を追加しました。

R12CCPU-V

2023 年 7 月 13 日

「対策方法」に対策済みの製品を追加しました。

R08/16/32/120SFCPU