MELSEC および 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 6 月 14 日
最終更新日 2024 年 5 月 30 日
三菱電機株式会社

■概要

MELSEC iQ-R/Q/L シリーズ CPU ユニットおよび MELIPC シリーズには、不適切なリソースロック(リソースの解放の不備)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、当該製品の 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-2022-24946)

この脆弱性の影響を受ける製品形名およびバージョンを以下に示します。

■CVSS スコア

CVE-2022-24946 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、シリアル No.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	R12CCPU-V	ファームウェアバージョン"16"以前
	Q シリーズ	Q03UDECPU、 Q04/06/10/13/20/26/50/100UDEHCPU	シリアル No.の上 5 桁"24061"以前
		Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"24051"以前
		Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"24051"以前
		Q12DCCPU-V、Q24DHCCPU-V(G)、 Q24/26DHCCPU-LS	シリアル No.の上 5 桁"25061"以前
	L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	シリアル No.の上 5 桁"24051"以前
MELIPC シリーズ		MI5122-VW	ファームウェアバージョン"05"以前

ファームウェアバージョンおよびシリアル No.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」の「付 1 製造情報・ファームウェアバージョン」
・「QCPU ユーザーズマニュアル(ハードウェア設計・保守点検編)」の「付 5 シリアル No.と機能バージョンの確認方法」
・「MELSEC-L CPU ユニットユーザーズマニュアル(ハードウェア設計・保守点検編)」の「付 5 シリアル No.と機能バージョンの確認方法」
・「MELIPC MI5000 シリーズ ユーザーズマニュアル(スタートアップ編) 」の「付 17 製造情報・ファームウェアバージョン」

■脆弱性の説明

MELSEC iQ-R/Q/L シリーズ CPU ユニットおよび MELIPC シリーズには、不適切なリソースロック(CWE-413)による 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 DoS 状態に陥ります。なお、復旧には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のうちファームウェアバージョン"08"以前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。
次項の通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。

<MELSEC iQ-R シリーズの該当製品のうちファームウェアバージョン"09"以降をご使用中のお客様>

次項に記載の対策済みバージョン以降へファームウェアをアップデートしてください。
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」

<MELSEC Q 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。
次項の通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ので、後継機種である MELSEC iQ-R シリーズへの移行もご検討ください。

〈MELSEC 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。
次項の通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ので、後継機種である MELSEC iQ-R シリーズへの移行もご検討ください。

〈MELIPC 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。
次項の通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	R12CCPU-V	ファームウェアバージョン"17"以降
	Q シリーズ	Q03UDECPU、 Q04/06/10/13/20/26/50/100UDEHCPU	シリアル No.の上 5 桁"24062"以降
		Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"24052"以降
		Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"24052"以降
		Q12DCCPU-V、Q24DHCCPU-V(G)、 Q24/26DHCCPU-LS	シリアル No.の上 5 桁"25062"以降
	L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	シリアル No.の上 5 桁"24052"以降
MELIPC シリーズ		MI5122-VW	ファームウェアバージョン"06"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。

■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 5 月 30 日
対策方法に関する内容を更新しました。

2023 年 7 月 27 日
「対策方法」に対策済みの製品として Q12DCCPU-V、Q24DHCCPU-V(G)、Q24/26DHCCPU-LS を追加しました。

2022 年 8 月 16 日
表題を該当製品に合わせて変更しました。
「該当製品の確認方法」に該当製品として R12CCPU-V、Q12DCCPU-V、Q24DHCCPU-V(G)、Q24/26DHCCPU-LS、MI5122-VW を追加しました。
「対策方法」に対策済みの製品として R12CCPU-V、Q03UDECPU、Q04/06/10/13/20/26/50/100UDEHCPU、MI5122-VW を追加しました。