MELSEC および MELIPC シリーズの Ethernet ポートにおける 複数のサービス拒否(DoS)の脆弱性

公開日 2021 年 11 月 30 日
最終更新日 2023 年 11 月 9 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、複数のサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、当該製品に対して不正なパケットを送信することにより、当該製品のプログラム実行または Ethernet 通信を停止させることができる可能性があります。(CVE-2021-20609、CVE-2021-20610、CVE-2021-20611)

■CVSS スコア [1]

・CVE-2021-20609 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5
・CVE-2021-20610 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5
・CVE-2021-20611 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、ファームウェアバージョン、シリアル No.および本体 OS ソフトウェア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	R00/01/02CPU	ファームウェアバージョン"24"以前※1
		R04/08/16/32/120(EN)CPU	ファームウェアバージョン"57"以前※1
		R08/16/32/120SFCPU	ファームウェアバージョン"26"以前※1
		R08/16/32/120PCPU	ファームウェアバージョン"29"以前※1
		R08/16/32/120PSFCPU	ファームウェアバージョン"08"以前※1
		R16/32/64MTCPU	本体 OS ソフトウェアバージョン"23"以前※6
		R12CCPU-V	ファームウェアバージョン"16"以前※1
	Q シリーズ	Q03UDECPU、Q04/06/10/13/20/26/50/100UDEHCPU	シリアル No.の上 5 桁"23121"以前※2
		Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"23071"以前※2
		Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"23071"以前※2
		Q12DCCPU-V、Q24DHCCPU-V(G)、Q24/26DHCCPU-LS	シリアル No.の上 5 桁"24031"以前※2
		MR-MQ100	本体 OS ソフトウェアバージョン"F"以前※3
		Q172/173DCPU-S1	本体 OS ソフトウェアバージョン"W"以前※4
		Q172/173DSCPU	本体 OS ソフトウェアバージョン"Y"以前※4
		Q170MCPU	本体 OS ソフトウェアバージョン"W"以前※5
		Q170MSCPU(-S1)	本体 OS ソフトウェアバージョン"Y"以前※8
	L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	シリアル No.の上 5 桁"23121"以前※2
MELIPC シリーズ		MI5122-VW	ファームウェアバージョン"05"以前※7

ファームウェアバージョン、シリアル No.および本体 OS ソフト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。
※1: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
※2: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
※3:MR-MQ100 User's Manual(Details)の 1.3 Combination of software version and a function
※4:Q173D(S)CPU/Q172D(S)CPU ユーザーズマニュアルの 2.2.2 本体 OS ソフトウェアバージョンの確認
※5:Q170MCPU ユーザーズマニュアルの 2.2.2 本体 OS ソフトウェアバージョンの確認
※6:MELSEC iQ-R モーションコントローラ ユーザーズマニュアルの 1.3 製造情報と本体 OS ソフトウェアバージョンの確認方法
※7: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
※8:Q170MSCPU(-S1)ユーザーズマニュアルの 2.2.2 本体 OS ソフトウェアバージョンの確認

■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、以下に示す複数のサービス拒否(DoS)の脆弱性が存在します。

・CVE-2021-20609: リソースの枯渇(CWE-400)[2]
・CVE-2021-20610: レングスパラメーターの不整合による不適切な処理(CWE-130)[3]
・CVE-2021-20611: 不適切な入力確認(CWE-20)[4]

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/400.html
3 https://cwe.mitre.org/data/definitions/130.html
4 https://cwe.mitre.org/data/definitions/20.html

■脆弱性がもたらす脅威
攻撃者には、不正なパケットを送信することにより、当該製品のプログラム実行または Ethernet 通信を停止できる可能性があります。なお、復旧には当該製品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	R00/01/02CPU	ファームウェアバージョン"25"以降
		R04/08/16/32/120(EN)CPU	ファームウェアバージョン"58"以降
		R08/16/32/120SFCPU	ファームウェアバージョン"27"以降
		R08/16/32/120PCPU	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
		R16/32/64MTCPU	本体 OS ソフトウェアバージョン"24"以降
		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"23122"以降
		Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"23072"以降
		Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"23072"以降
		Q12DCCPU-V、Q24DHCCPU-V(G)、Q24/26DHCCPU-LS	シリアル No.の上 5 桁"24032"以降
		MR-MQ100	本体 OS ソフトウェアバージョン"G"以降
		Q172/173DCPU-S1	本体 OS ソフトウェアバージョン"X"以降
		Q172/173DSCPU	本体 OS ソフトウェアバージョン"Z"以降
		Q170MCPU	本体 OS ソフトウェアバージョン"X"以降
		Q170MSCPU(-S1)	本体 OS ソフトウェアバージョン"Z"以降
	L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	シリアル No.の上 5 桁"23122"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。
・リモートパスワード機能または IP フィルタ機能※9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。
※9:リモートパスワード機能および 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「リモートパスワード」「IP フィルタ」
MELSEC iQ-R モーションコントローラ プログラミングマニュアルの 6.2 セキュリティ機能の「IP フィルタ機能」
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」
QnUCPU ユーザーズマニュアル(内蔵 Ethernet ポート通信編)の「第 10 章リモートパスワード」
MELSEC-L CPU ユニット ユーザーズマニュアル(内蔵 Ethernet 機能編)の「第 11 章リモートパスワード」
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
2023 年 11 月 9 日
「対策方法」に対応済みの製品を追加しました。
Q172/173DSCPU、Q170MSCPU(-S1)

2023 年 4 月 24 日
影響を受けるバージョンと対策済みバージョンを修正しました。
R08/16/32/120SFCPU

2022 年 11 月 24 日
「対策方法」に対応済みの製品を追加しました。
R08/16/32/120SFCPU

2022 年 7 月 26 日
「対策方法」に対応済みの製品を追加しました。
R12CCPU-V、MI5122-VW

2022 年 5 月 31 日
「対策方法」に対応済みの製品を追加しました。
R08/16/32/120PSFCPU、R16/32/64MTCPU

2022 年 4 月 26 日
「対策方法」に対応済みの製品を追加しました。
Q12DCCPU-V、Q24DHCCPU-V(G)、Q24/26DHCCPU-LS、MR-MQ100、Q172/173DCPU-S1、Q170MCPU

2022 年 1 月 27 日
「対策方法」に対応済みの製品を追加しました。
Q03UDECPU、Q04/06/10/13/20/26/50/100UDEHCPU、L02/06/26CPU(-P)、L26CPU-(P)BT
「該当製品の確認方法」の製品名を修正しました。
Q172/173DSCPU