MELSEC iQ-R、Q および L シリーズ CPU ユニットの Ethernet ポートにおけるサービス拒否(DoS)の脆弱性

公開日 2020 年 10 月 29 日
最終更新日 2023 年 12 月 19 日
三菱電機株式会社

■概要

MELSEC iQ-R、Q および L シリーズの CPU ユニットには、リソース枯渇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、Ethernet 通信が DoS 状態に陥る可能性があります。(CVE-2020-5652)

この脆弱性の影響を受ける製品形名およびファームウェアバージョンを以下に示します。

■CVSS スコア

CVE-2020-5652 CVSS:3.0/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

MELSEC iQ-R、Q および L シリーズの CPU ユニットのうち、次の製品形名とファームウェアバージョン、本体 OS ソフトウェアバージョン又はシリアル No.のものが影響を受けます。

シリーズ	形名	バージョン
iQ-R シリーズ	R00/01/02CPU	ファームウェアバージョン"20"以前
	R04/08/16/32/120(EN)CPU	ファームウェアバージョン"52"以前
	R08/16/32/120SFCPU	ファームウェアバージョン"22"以前
	R08/16/32/120PCPU	ファームウェアバージョン"25"以前
	R16/32/64MTCPU	本体 OS ソフトウェアバージョン"21"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"22081"以前
	Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"22031"以前
	Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"22031"以前
	Q172/173DCPU-S1	本体 OS ソフトウェアバージョン"V"以前
	Q172/173DSCPU	本体 OS ソフトウェアバージョン"W"以前
	Q170MCPU	本体 OS ソフトウェアバージョン"V"以前
	Q170MSCPU(-S1)	本体 OS ソフトウェアバージョン"W"以前
L シリーズ	L02/06/26CPU(-P)、 L26CPU-(P)BT	シリアル No.の上 5 桁"23121"以前

ファームウェアバージョン、本体 OS ソフトウェアバージョンおよびシリアル No.の確認方法は、各製品のマニュアルをご参照ください。

■脆弱性の説明

MELSEC iQ-R、Q および L シリーズの CPU ユニットには、リソース枯渇(CWE-400)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 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。

■対策方法

下記ユニットにおいては、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しています。

シリーズ	形名	バージョン
iQ-R シリーズ	R00/01/02CPU	ファームウェアバージョン"21"以降
	R04/08/16/32/120(EN)CPU	ファームウェアバージョン"53"以降
	R08/16/32/120SFCPU	ファームウェアバージョン"23"以降
	R08/16/32/120PCPU	ファームウェアバージョン"26"以降
	R16/32/64MTCPU	本体 OS ソフトウェアバージョン"22"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"22082"以降
	Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"22032"以降
	Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"22032"以降
	Q172/173DCPU-S1	本体 OS ソフトウェアバージョン"W"以降
	Q172/173DSCPU	本体 OS ソフトウェアバージョン"X"以降
	Q170MCPU	本体 OS ソフトウェアバージョン"W"以降
	Q170MSCPU(-S1)	本体 OS ソフトウェアバージョン"X"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

■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。

・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。

■謝辞

本脆弱性をご報告いただいた、ZheJiangQiAnTechnology の joker63 様に感謝いたします。

■お客様からのお問い合わせ先

お客様からのお問い合わせ先につきましては、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 12 月 19 日
謝辞を追加しました。

2022 年 3 月 29 日
「該当製品の確認方法」及び「対策方法」に対応済み製品の情報を追加しました。

2022 年 1 月 13 日
「対策方法」に対応済みの製品を追加しました。

2021 年 5 月 18 日
R08/16/32/120PCPU の対策方法の情報を追加しました。
R08/16/32/120PSFCPU を該当製品から削除しました。