MELSEC iQ-R 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 2020 年 10 月 8 日
最終更新日 2024 年 8 月 22 日
三菱電機株式会社

■概要

MELSEC iQ-R シリーズのユニットには、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、CPU ユニットでエラーが発生し、プログラム実行および通信が DoS 状態に陥る可能性があります。(CVE-2020-16850)

この脆弱性の影響を受ける製品形名並びにファームウェアバージョンおよび本体 OS ソフトウェアバージョンを以下に示します。

■CVSS スコア [1]

CVE-2020-16850 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

MELSEC iQ-R シリーズのユニットのうち、次の製品形名とファームウェアバージョン又は本体 OS ソフトウェアバージョンのものが影響を受けます。

・R00/01/02CPU:ファームウェアバージョン"20"以前
・R04/08/16/32/120CPU、R04/08/16/32/120ENCPU: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

ファームウェアバージョンおよび本体 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。
・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-R モーションコントローラ ユーザーズマニュアル「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」
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 シリーズのユニットには、リソース枯渇(CWE-400)[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

攻撃者から不正なパケットを受信すると、CPU ユニットでエラーが発生し、プログラム実行および通信が 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

以下の表を参照し、ご使用中の製品がアップデート可能かどうかをご確認ください

シリーズ	形名	アップデート可否
iQ-R シリーズ	R00/01/02CPU	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」を参照ください。
	R04/08/16/32/120CPU、 R04/08/16/32/120ENCPU	
	R08/16/32/120SFCPU	
	R08/16/32/120PCPU	
	R16/32/64MTCPU	全バージョンでアップデート可能

〈アップデートが可能な場合〉

以下のサイトから、「■製品での対応」に記載の対策済みバージョンのアップデート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
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 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(共通編)「8.4 本体 OS ソフトウェアのインストール」

〈アップデートが不可な場合〉

該当製品・該当バージョンをご使用中のお客様は、軽減策・回避策にて対応ください。
「■製品での対応」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://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/400.html

■製品での対応

下記ユニットにおいては、対策を実施済みです。

・R00/01/02CPU：ファームウェアバージョン"21"以降
・R04/08/16/32/120CPU、R04/08/16/32/120ENCPU：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

■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。
・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

この問題をご報告いただいた SCADAfence Ltd 社 Yossi Reuven 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

2024 年 8 月 22 日

R08/16/32/120PSFCPU を「該当製品の確認方法」及び「対策方法」から削除しました。
「CVSS スコア」を追加しました。
「お客様での対応」を追加しました。
「対策方法」を「製品での対応」に変更しました。
「概要」に本体 OS ソフトウェアバージョンを追加しました。
R16/32/64MTCPU の「該当製品の確認方法」、「製品での対応」について、ファームウェアバージョンを本体 OS ソフトウェアバージョンに修正しました。

2021 年 5 月 18 日

「影響を受ける製品」に R08/16/32/120PSFCPU を追加しました。
R16/32/64MTCPU の対策方法の情報を追加しました。

2021 年 2 月 18 日

「対策方法」に対応済みの製品を追加しました。

2020 年 10 月 26 日

「対策方法」に対応済みの製品を追加しました。