MELSEC シリーズ CPU ユニットにおけるサービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性

公開日 2023 年 5 月 23 日
最終更新日 2024 年 4 月 25 日
三菱電機株式会社

■概要

MELSEC シリーズの CPU ユニットには、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在します。攻撃者は、該当製品に対して不正なパケットを送信することにより、当該製品をサービス停止(DoS)状態に陥らせたり、悪意のあるプログラムを実行させたりすることができる可能性があります。ただし、悪意のあるプログラムを実行するためには、攻撃者は、製品の内部構造を知る必要があるため、悪意のあるプログラムを実行することは、容易ではありません。(CVE-2023-1424)

■CVSS スコア [1]

CVE-2023-1424 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H 基本値 10.0

■該当製品の確認方法

影響を受ける製品とバージョンは以下のとおりです。

シリーズ	製品形名		ファームウェアバージョン
MELSEC iQ-F シリーズ	FX5U-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS	製造番号 17X****以降	1.220 以降～1.281 以前
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	製造番号 17X****以降	
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		
MELSEC iQ-R シリーズ	R00/01/02CPU		35 以前
	R04/08/16/32/120(EN)CPU		12 以降～68 以前
	R08/16/32/120SFCPU		26 以降～31 以前
	R08/16/32/120PCPU		3 以降～37 以前

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-F FX5S/FX5UJ/FX5U/FX5UC ユーザーズマニュアル(ハードウェア編)
17.3 エンジニアリングツールによる確認 「ユニット診断」

・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」

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 シリーズの CPU ユニットには、古典的バッファオーバーフロー(CWE-120[2])により、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在します。

■脆弱性がもたらす脅威

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、当該製品をサービス停止(DoS)状態に陥らせたり、悪意のあるプログラムを実行できる可能性があります。ただし、悪意のあるプログラムを実行するためには、攻撃者は、製品の内部構造を知る必要があるため、悪意のあるプログラムを実行することは、容易ではありません。なお、サービス停止(DoS)状態からの復旧及び悪意のあるプログラムが実行された場合の復旧には当該製品のリセットが必要です。

■お客様での対応

<MELSEC iQ-F シリーズの該当製品をご使用中のお客様>
以下のサイトより、次項に記載の対策済みバージョンのファームウェア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-F FX5 ユーザーズマニュアル(応用編)「第 9 章 ファームウェアアップデート機能」

<MELSEC iQ-R シリーズ R08/16/32/120SFCPU の該当製品をご使用中のお客様>
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。

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/120.html

〈上記以外の MELSEC iQ-R シリーズの該当製品をご使用中のお客様〉
以下のサイトより、次項に記載の対策済みバージョンのファームウェア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」

■製品での対応
以下のバージョンで対策済みです。

シリーズ	製品形名		ファームウェアバージョン
MELSEC iQ-F シリーズ	FX5U-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS	製造番号 17X****以降	1.290 以降
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	製造番号 17X****以降	
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		
MELSEC iQ-R シリーズ	R00/01/02CPU		36 以降
	R04/08/16/32/120(EN)CPU		69 以降
	R08/16/32/120SFCPU		32 以降
	R08/16/32/120PCPU		38 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※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。
・当該製品が接続された LAN への物理的なアクセスを制限してください。

※:IP フィルタ機能については、以下のマニュアルを参照ください。
MELSEC iQ-F FX5 ユーザーズマニュアル(通信編)「13.1 IP フィルタ機能」
MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編)「1.13 セキュリティ」の「IP フィルタ」

■謝辞
本脆弱性をご報告いただいた、Cisco Talos の Matt Wiseman 様に感謝いたします。

■お客様からのお問い合わせ先
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 4 月 25 日
「対策方法」を「お客様での対応」と「製品での対応」に分けました。

2024 年 3 月 14 日
「対策方法」に対策済みの製品として、R08/16/32/120SFCPU を追加しました。

2023 年 9 月 12 日
「対策方法」に対策済みの製品として、R08/16/32/120PCPU を追加しました。

2023 年 7 月 6 日
「該当製品の確認方法」に該当製品として、MELSEC iQ-R シリーズのユニットを追加しました。
「対策方法」に対策済みの製品として、R00/01/02CPU,R04/08/16/32/120(EN)CPU を追加しました。