MELSEC シリーズの WEB サーバ機能における認証回避の脆弱性

公開日 2023 年 1 月 17 日
最終更新日 2023 年 4 月 18 日
三菱電機株式会社

■概要

MELSEC iQ-F/iQ-R シリーズの WEB サーバ機能において、認証回避の脆弱性が存在することが判明しました。攻撃者は、収集した使用済みの乱数から認証に使用される乱数を推測することで、認証を回避して WEB サーバ機能へ不正にアクセスできる可能性があります。(CVE-2022-40267)

この脆弱性の影響を受ける製品形名及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 [1]

CVE-2022-40267 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値 5.9

■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通りです。

シリーズ	製品形名		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	1.280 以前
		製造番号 179****以前	1.074 以前
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	製造番号 17X****以降	1.280 以前
		製造番号 179****以前	1.074 以前
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		1.280 以前
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,ESS		1.042 以前
	FX5S-xMy/z x=30,40,60,80, y=T,R, z=ES,ESS		1.003 以前
MELSEC iQ-R シリーズ	R00/01/02CPU		33 以前
	R04/08/16/32/120(EN)CPU		66 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)
15.3 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」
各種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-F/iQ-R シリーズの CPU ユニットには、疑似乱数生成器における予測可能なシード(CWE-337[2])により、認証回避の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者が、収集した使用済みの乱数から認証に使用される乱数を推測することで、認証を回避して WEB サーバ機能へ不正にアクセスできる可能性があります。

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/337.html

■対策方法

以下のバージョンで対策済みです。

シリーズ	製品形名		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	1.281 以降
		製造番号 179****以前	1.075 以降
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	製造番号 17X****以降	1.281 以降
		製造番号 179****以前	1.075 以降
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		1.281 以降
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,ESS		1.044 以降
	FX5S-xMy/z x=30,40,60,80, y=T,R, z=ES,ESS		1.004 以降
MELSEC iQ-R シリーズ	R00/01/02CPU		34 以降
	R04/08/16/32/120(EN)CPU		67 以降

以下のサイトより対策済みのバージョンのファームウェアアップデート情報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

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)「5 ファームウェアアップデート機能」

・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」

■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。

※: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(Ethernet 通信編)「12.1 IP フィルタ機能」

MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編)の「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

2023 年 4 月 18 日

「対策方法」に対策済みの製品を追加しました。

R00/01/02CPU、R04/08/16/32/120(EN)CPU

2023 年 2 月 28 日

「該当製品の確認方法」に該当製品として、FX5S CPU 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、FX5SCPU ユニットを追加しました。

2023 年 1 月 26 日

「該当製品の確認方法」に該当製品として、FX5UJ CPU 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、FX5UJ CPU ユニットを追加しました。