MELSEC シリーズにおける情報漏えいの脆弱性

公開日 2023 年 3 月 2 日
最終更新日 2023 年 6 月 20 日
三菱電機株式会社

■概要

MELSEC iQ-F、iQ-R、Q、L シリーズにおいて、情報漏えいの脆弱性が存在することが判明しました。攻撃者が、プロジェクトファイル内に平文で保存された認証情報を入手することにより、FTP サーバ機能や Web サーバ機能に不正にログインできる可能性があります。(CVE-2023-0457)

■CVSS スコア [1]

CVE-2023-0457 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値 7.5

■該当製品の確認方法

影響を受ける製品は、以下のとおりです。

シリーズ	製品名	バージョン
MELSEC iQ-F シリーズ	FX5U(C) CPU ユニット 全機種	全バージョン
	FX5UJ CPU ユニット 全機種	全バージョン
	FX5S CPU ユニット 全機種	全バージョン
	FX5-ENET	全バージョン
	FX5-ENET/IP	全バージョン
MELSEC iQ-R シリーズ	R00/01/02CPU	全バージョン
	R04/08/16/32/120(EN)CPU	全バージョン
	R08/16/32/120SFCPU	全バージョン
	R08/16/32/120PCPU	全バージョン
	R08/16/32/120PSFCPU	全バージョン
	RJ71EN71	全バージョン
	R12CCPU-V	全バージョン
MELSEC-Q シリーズ	Q03UDECPU、Q04/06/10/13/20/26/50/100UDEHCPU	全バージョン
	Q03/04/06/13/26UDVCPU	全バージョン
	Q04/06/13/26UDPVCPU	全バージョン
	QJ71E71-100	全バージョン
MELSEC-L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	全バージョン
	LJ71E71-100	全バージョン

■脆弱性の説明

MELSEC iQ-F、iQ-R、Q、L シリーズには、認証情報の平文保存(CWE-256[2])による、情報漏えいの脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者が、プロジェクトファイル内に平文で保存された認証情報を入手することにより、FTP サーバ機能や Web サーバ機能に不正にログインできる可能性があります。

■対策方法

軽減策・回避策にて対応をお願いいたします。

■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。

・プロジェクトファイルの送受信や共有をする場合は、当該ファイルや通信データを暗号化してください。
・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。
・MELSEC iQ-F、iQ-R シリーズにおいては、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(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」

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/256.html

■謝辞

本脆弱性をご報告いただいた、HelloT の JeongHoon Bae 様、YiJoon Jung 様、JinYoung Kim 様、HyeokJong Yun 様、HeeA Go 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 6 月 20 日
「該当製品の確認方法」に該当製品として、MELSEC iQ-R、Q、L シリーズのユニットを追加しました。