複数の FA 製品における認証回避、情報漏えい及び情報改ざんの脆弱性

公開日 2022 年 3 月 31 日
最終更新日 2022 年 5 月 31 日
三菱電機株式会社

■概要

三菱電機製の複数の FA 製品において、認証回避、情報漏えい及び情報改ざんの脆弱性が存在することが判明しました。これらの脆弱性を悪意のある攻撃者に悪用された場合に、当該製品への不正ログイン若しくは当該製品の情報の漏えい又は改ざんが発生する可能性があります。(CVE-2022-25155、CVE-2022-25156、CVE-2022-25157、CVE-2022-25158、CVE-2022-25159、CVE-2022-25160)

■CVSS スコア

CVE-2022-25155	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	基本値 5.9
CVE-2022-25156	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	基本値 5.9
CVE-2022-25157	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N	基本値 7.4
CVE-2022-25158	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N	基本値 7.4
CVE-2022-25159	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	基本値 5.9
CVE-2022-25160	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N	基本値 6.8

■該当製品の確認方法

影響を受ける製品は、以下の通りです。

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
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
	R16/32/64MTCPU (※1)	全バージョン
	RJ71GN11-T2 (※2)	全バージョン
	RJ71GN11-EIP (※2)	全バージョン
	RJ71C24(-R2/R4)	全バージョン
	RJ71EN71	全バージョン
	RJ71GF11-T2 (※3)	全バージョン
	RJ71GP21(S)-SX (※3)	全バージョン
	RJ72GF15-T2	全バージョン
MELSEC Q シリーズ	Q03UDECPU、Q04/06/10/13/20/26/50/100UDEHCPU (※4)	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
	QJ71C24N(-R2/R4)	全バージョン
	QJ71E71-100	全バージョン
	QJ72BR15 (※5)	全バージョン
	QJ72LP25(-25/G/GE) (※5)	全バージョン
MELSEC L シリーズ (※4)	L02/06/26CPU(-P)、L26CPU-(P)BT	全バージョン
	LJ71C24(-R2)	全バージョン
	LJ71E71-100	全バージョン
	LJ72GF15-T2	全バージョン

※1 CVE-2022-25157/25159/25160 のみ該当
※2 CVE-2022-25155 のみ該当
※3 CVE-2022-25157/25158 のみ該当
※4 CVE-2022-25155/25156/25157/25158 のみ該当
※5 CVE-2022-25155/25156 のみ該当

■脆弱性の説明

三菱電機製の複数の FA 製品には、以下の脆弱性が存在します。

CVE-2022-25155: パスワードの代わりにパスワードハッシュを使用する認証(CWE-836)
CVE-2022-25156: 脆弱なハッシュアルゴリズムの使用(CWE-328)
CVE-2022-25157: パスワードの代わりにパスワードハッシュを使用する認証(CWE-836)
CVE-2022-25158: 重要な情報の平文保存(CWE-312)
CVE-2022-25159: キャプチャリプレイによる認証回避(CWE-294)

CVE-2022-25160: 重要な情報の平文保存（CWE-312）

■脆弱性がもたらす脅威

これらの脆弱性を悪意のある攻撃者に悪用された場合、当該製品への不正ログイン若しくは当該製品の情報の漏えい又は改ざんが発生す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。

- 信頼できないネットワークやホストを経由した通信を行う場合は、仮想プライベートネットワーク(VPN)の設置により通信経路を暗号化してください。
- ファイアウォール、IP フィルタ機能などを使用し、当該製品への接続を最小限に抑え、信頼できないネットワークやホストからアクセスできないようにしてください。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)の 「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」
  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)の「6.2 セキュリティ機能」の「IP フィルタ機能」
  MELSEC iQ-R CC-Link IE TSN ユーザーズマニュアル(応用編)の「1.4 セキュリティ」の「IP フィルタ」
  MELSEC iQ-R CC-Link IE TSN Plus マスタ・ローカルユニットユーザーズマニュアルの「9.5 セキュリティ」の「IP フィルタ」
  Q 対応 Ethernet インタフェースユニット ユーザーズマニュアル（基本編）の「14.3 IP フィルタ機能」
  MELSEC-L Ethernet インタフェースユニット ユーザーズマニュアル（基本編）の「14.3 IP フィルタ機能」

■謝辞

本脆弱性をご報告いただいた、Positive Technologies 社の以下の皆様に感謝いたします。
CVE-2022-25155: Anton Dorfman 様
CVE-2022-25156: Dmitry Sklyarov 様、Anton Dorfman 様
CVE-2022-25157: Anton Dorfman 様
CVE-2022-25158: Anton Dorfman 様、Iliya Rogachev 様
CVE-2022-25159: Anton Dorfman 様
CVE-2022-25160: Anton Dorfman 様、Artur Akhatov 様

■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

2022 年 5 月 31 日
「該当製品の確認方法」に MELSEC iQ-R/Q/L シリーズの対象製品を追加しました。
「軽減策・回避策」に MELSEC iQ-R/Q/L シリーズの対象マニュアルの情報を追加しました。