複数の FA エンジニアリングソフトウェア製品における複数の脆弱性

公開日 2022 年 11 月 24 日
最終更新日 2023 年 12 月 12 日
三菱電機株式会社

■概要

三菱電機製の複数の FA エンジニアリングソフトウェア製品において、複数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、当該製品の情報の漏えい又は改ざんにより、結果として、権限のないユーザに MELSEC iQ-R/F/L シリーズの CPU ユニット及び MELSEC iQ-R シリーズ OPC UA サーバユニットへアクセスされる可能性や、プログラムを不正に閲覧、実行される可能性、プロジェクトファイルを不正に閲覧される可能性があります。(CVE-2022-25164、CVE-2022-29825、CVE-2022-29826、CVE-2022-29827、CVE-2022-29828、CVE-2022-29829、CVE-2022-29830、CVE-2022-29831、CVE-2022-29832、CVE-2022-29833)

■CVSS スコア [1]

CVE-2022-25164 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N 基本値:8.6
CVE-2022-29825 CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N 基本値:5.6
CVE-2022-29826 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N 基本値:6.8
CVE-2022-29827 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N 基本値:6.8
CVE-2022-29828 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N 基本値:6.8
CVE-2022-29829 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N 基本値:6.8
CVE-2022-29830 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N 基本値:9.1
CVE-2022-29831 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値:7.5
CVE-2022-29832 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N 基本値:3.7
CVE-2022-29833 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N 基本値:6.8

[1] https://www.ipa.go.jp/security/vuln/CVSSv3.html

■該当製品の確認方法

〈製品とバージョン〉

No.	製品名	バージョン	該当 CVE 番号
1	GX Works3	1.000A 以降 1.011M 以前	CVE-2022-25164 CVE-2022-29825 CVE-2022-29826 CVE-2022-29827 CVE-2022-29828 CVE-2022-29829 CVE-2022-29830
		1.015R 以降 1.087R 以前	CVE-2022-25164 CVE-2022-29825 CVE-2022-29826 CVE-2022-29827 CVE-2022-29828 CVE-2022-29829 CVE-2022-29830 CVE-2022-29831 CVE-2022-29832 CVE-2022-29833
		1.090U	CVE-2022-25164 CVE-2022-29825 CVE-2022-29827 CVE-2022-29828 CVE-2022-29829 CVE-2022-29830 CVE-2022-29831 CVE-2022-29832 CVE-2022-29833
		1.095Z	CVE-2022-25164 CVE-2022-29827 CVE-2022-29828 CVE-2022-29830 CVE-2022-29831 CVE-2022-29832 CVE-2022-29833
		1.096A 以降	CVE-2022-29827 CVE-2022-29828 CVE-2022-29832 CVE-2022-29833
2	MX OPC UA Module Configurator-R	1.08J 以前	CVE-2022-25164
3	GX Works2	全て	CVE-2022-29832
4	GX Developer	8.40S 以降	CVE-2022-29832
5	GT Designer3 Version1 (GOT2000)	1.122C 以降 1.290C 以前	CVE-2022-29825 CVE-2022-29829
6	モーション制御設定(*1)	1.000A 以降 1.033K 以前	CVE-2022-29826 CVE-2022-29830
		1.035M 以降 1.042U 以前	CVE-2022-29826 CVE-2022-29829 CVE-2022-29830
		1.045X 以降	CVE-2022-29830

(*1) GX Works3 関連ソフトウェア

〈バージョンの確認方法〉

・GX Works3 : 「GX Works3 オペレーティングマニュアル」の「1.8 GX Works3 の操作方法について調べる」の「GX Works3 のバージョン確認」を参照ください。

・MX OPC UA Module Configurator-R : 「MELSEC iQ-R OPC UA サーバユニットユーザーズマニュアル(応用編)」の「2.12 ヘルプ」を参照ください。

・GX Works2 : 「GX Works2 Version 1 オペレーティングマニュアル(共通編)」の「3.4.4 GX Works2 のバージョンを確認する」を参照ください。

・GX Developer : 「GX Developer Version 8 オペレーティングマニュアル」の「15.18 ヘルプ概要」を参照ください。

・GT Designer3 Version1 (GOT2000) : 「GT Designer3 (GOT2000) 画面設計マニュアル」の「2.2 GT Designer3 の画面構成」で[メニュー構成]の[ヘルプ]を参照ください。

・モーション制御設定 ：「モーション制御設定機能ヘルプ」の「1.2 モーション制御設定機能の操作方法について調べる」の「モーション制御設定機能のバージョン確認」を参照ください。

〈マニュアルの入手方法〉
以下サイトよりソフトウェア製品の最新のマニュアルをダウンロードいただけます。
https://www.mitsubishielectric.co.jp/fa/download/index.html

■脆弱性の説明
三菱電機製の複数の FA エンジニアリングソフトウェア製品には、以下の脆弱性が存在します。
CVE-2022-25164：重要な情報の平文保存(CWE-312)[2]による情報漏えいの脆弱性
CVE-2022-29825：ハードコードされたパスワードの使用(CWE-259)[3]による情報漏えいの脆弱性
CVE-2022-29826：重要な情報の平文保存(CWE-312)による情報漏えいの脆弱性
CVE-2022-29827：ハードコードされた暗号鍵の使用(CWE-321)[4]による情報漏えいの脆弱性
CVE-2022-29828：ハードコードされた暗号鍵の使用(CWE-321)による情報漏えいの脆弱性
CVE-2022-29829：ハードコードされた暗号鍵の使用(CWE-321)による情報漏えいの脆弱性
CVE-2022-29830：ハードコードされた暗号鍵の使用(CWE-321)による情報漏えい及び情報改ざんの脆弱性
CVE-2022-29831：ハードコードされたパスワードの使用(CWE-259)による情報漏えいの脆弱性
CVE-2022-29832：メモリにおける平文での重要な情報の保存(CWE-316)[5]による情報漏えいの脆弱性
CVE-2022-29833：認証情報の不十分な保護(CWE-522)[6]による情報漏えいの脆弱性

■脆弱性がもたらす脅威
CVE-2022-25164：
本脆弱性が悪用された場合、機密情報が漏洩する恐れがあります。結果として、権限のないユーザによって CPU ユニット及び OPC UA サーバユニットへ不正にアクセスされる可能性があります。
CVE-2022-29825、CVE-2022-29826、CVE-2022-29827、CVE-2022-29828、CVE-2022-29829：
これらの脆弱性が悪用された場合、機密情報が漏洩する恐れがあります。結果として、権限のないユーザによってプログラム及びプロジェクトファイルの不正な閲覧やプログラムの不正な実行が行われる可能性があります。
CVE-2022-29830：
本脆弱性が悪用された場合、機密情報が漏洩又は改ざんされる恐れがあります。結果として、権限のないユーザによってプロジェクトファイルに関する情報を不正に取得される可能性があります。
CVE-2022-29831：
本脆弱性が悪用された場合、権限のないユーザによって安全 CPU ユニットのプロジェクトファイルに関する情報が漏えいする恐れがあります。
CVE-2022-29832：
本脆弱性が悪用された場合、機密情報が漏えいする恐れがあります。結果として、権限のないユーザによって安全 CPU のプロジェクトファイル及び MELSEC Q/FX/L シリーズのセキュリティ設定したプロジェクトファイルに関する情報を不正に取得される可能性があります。
CVE-2022-29833：
本脆弱性が悪用された場合、機密情報が漏えいする恐れがあります。結果として、権限のないユーザによって安全 CPU ユニットへ不正にアクセスされる可能性があります。

■対策方法
脆弱性ごとの対策方法を下表に示します。
なお、対策方法の記載がない製品(GX Works2 及び GX Developer)やすぐに製品をアップデート出来ない場合には、軽減策・回避策にて対応をお願いいたします。
対策品にアップデートする場合には、〈対策品の入手方法〉及び〈アップデート方法〉を参考にしてください。

2 https://cwe.mitre.org/data/definitions/312.html
3 https://cwe.mitre.org/data/definitions/259.html
4 https://cwe.mitre.org/data/definitions/321.html
5 https://cwe.mitre.org/data/definitions/316.html
6 https://cwe.mitre.org/data/definitions/522.html

No.	製品名	該当 CVE 番号	対策方法
1	GX Works3	CVE-2022-29826	Ver. 1.090U 以降にアップデートしてください。
		CVE-2022-29825 CVE-2022-29829	Ver. 1.095Z 以降にアップデートし、セキュリティキーのセキュアモードを「有効」に設定してください。 詳細は、「GX Works3 オペレーティングマニュアル」の「15.2 プログラムの不正な閲覧の防止(セキュリティキー)」を参照して下さい。
		CVE-2022-25164 CVE-2022-29830 CVE-2022-29831	Ver. 1.096A 以降にアップデートし、プロジェクトのセキュリティバージョンを「2」に設定してください。 詳細は、「GX Works3 オペレーティングマニュアル」の「15.8 データの不正な閲覧/改ざんの防止(セキュリティバージョン)」を参照して下さい。
		CVE-2022-29827 CVE-2022-29828 CVE-2022-29832 CVE-2022-29833	軽減策・回避策にて対応をお願いいたします。
2	MX OPC UA Module Configurator-R	CVE-2022-25164	Ver.1.09K 以降にアップデートしてください。 また、OPC UA サーバユニットのファームウェアバージョンを 10 以降にアップデートしてください。
3	GT Designer3 Version1 (GOT2000)	CVE-2022-29825 CVE-2022-29829	Ver. 1.295H 以降にアップデートし、セキュリティキーのセキュアモードを「有効」に設定してください。 詳細は、「GT Designer3 (GOT2000) 画面設計マニュアル」の「2.12 セキュリティキーでプロジェクトを保護する」で[セキュリティキー管理]ダイアログの[セキュアモード切替え]ダイアログを参照してください。
4	モーション制御設定	CVE-2022-29826	Ver.1.045X 以降にアップデートしてください。 また、本表 No.1 GX Works3 の CVE-2022-29826 の対策方法を実施してください。
		CVE-2022-29829	Ver.1.045X 以降にアップデートしてください。 また、本表 No.1 GX Works3 の CVE-2022-29829 の対策方法を実施してください。
		CVE-2022-29830	軽減策・回避策にて対応をお願いいたします。

<対策品の入手方法>
以下サイトよりソフトウェア製品の最新版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

<アップデート方法>
1. ダウンロードしたファイル(zip 形式)を解凍します。
2. 解凍されたフォルダ中の setup.exe を実行してインストールを行ってください。

■軽減策・回避策
これらの脆弱性が悪用され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・回避策を講じることを推奨します。

該当 CVE 番号	軽減策・回避策
CVE-2022-25164	・コンピュータ/サーバ内のプロジェクトファイルやセキュリティキー、及び当該製品をインストールしているパソコン内の設定ファイルが、悪意ある第三者に取得されないように、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する。 ・当該製品を使用するパソコンにウイルス対策ソフトを搭載する。 ・プロジェクトファイルやセキュリティキーをインターネット経由で送受信する場合、当該ファイルを暗号化する。 ・OPC UA クライアントから MELSEC iQ-R シリーズ OPC UA サーバユニットへのアクセスに対するユーザ認証を、「ユーザ名/パスワードによる認証」ではなく、「証明書による認証」機能を使用する。(MX OPC UA ModuleConfigurator-R のみ)
CVE-2022-29825	・コンピュータ/サーバ内のプロジェクトファイルやセキュリティキー、及び当該製品をインストールしているパソコン内の設定ファイルが、悪意ある第三者に取得されないように、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する。 ・当該製品を使用するパソコンにウイルス対策ソフトを搭載する。
CVE-2022-29826 CVE-2022-29827 CVE-2022-29828 CVE-2022-29829 CVE-2022-29830 CVE-2022-29831 CVE-2022-29832 CVE-2022-29833	・コンピュータ/サーバ内のプロジェクトファイルやセキュリティキー、及び当該製品をインストールしているパソコン内の設定ファイルが、悪意ある第三者に取得されないように、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する。 ・当該製品を使用するパソコンにウイルス対策ソフトを搭載する。 ・プロジェクトファイルやセキュリティキーをインターネット経由で送受信する場合、当該ファイルを暗号化する。

■謝辞

これらの脆弱性をご報告いただいた以下の皆様に感謝いたします。

CVE-2022-25164: Positive Technologies 社 Anton Dorfman 様, Vladimir Nazarov 様
CVE-2022-29825: Positive Technologies 社 Anton Dorfman 様, Dmitry Sklyarov 様
CVE-2022-29826: Positive Technologies 社 Anton Dorfman 様, Iliya Rogachev 様
CVE-2022-29827: Positive Technologies 社 Dmitry Sklyarov 様, Anton Dorfman 様
CVE-2022-29828: Positive Technologies 社 Dmitry Sklyarov 様, Anton Dorfman 様
CVE-2022-29829: Positive Technologies 社 Dmitry Sklyarov 様, Anton Dorfman 様
CVE-2022-29830: Positive Technologies 社 Dmitry Sklyarov 様, Anton Dorfman 様
CVE-2022-29831: Nozomi Networks 社 Ivan Speziale 様
CVE-2022-29832: Nozomi Networks 社 Ivan Speziale 様
CVE-2022-29833: Nozomi Networks 社 Ivan Speziale 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

2023 年 12 月 12 日
・「対策方法」に対策版を提供する予定のない製品名(GX Works2 及び GX Developer)を追記しました。

2023 年 6 月 29 日
・「該当製品の確認方法」において以下の製品の該当バージョンを修正しました。
GX Works3、MX OPC UA Module Configurator-R
・「対策方法」に GX Works3 の対策方法の情報を追加しました。
・「対策方法」に MX OPC UA Module Configurator-R を追加しました。

2023 年 5 月 30 日
・「該当製品の確認方法」に以下の製品を追加しました。
GX Works2
GX Developer
GT Designer3 Version1 (GOT2000)
モーション制御設定
・上記に伴い、「概要」及び「脆弱性がもたらす脅威」を修正しました。
・「脆弱性の説明」に脆弱性の概説を追記しました。
・「対策方法」に対策済みの製品を追加しました。