複数の FA エンジニアリングソフトウェア製品における XML 処理の不備に起因する脆弱性

公開日 2020 年 6 月 30 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ついて、XML 処理の不備に起因する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用された場合、悪意ある第三者の攻撃により、該当のソフトウェア製品が動作しているコンピュータ上のファイルが外部に送信される、もしくは該当のソフトウェア製品がサービス拒否(DoS)状態に陥る危険性があります。
この問題の影響を受けるソフトウェア製品名およびバージョンを以下に示しますので、対策済バージョンにアップデートしてください。

■該当製品の確認方法

<製品とバージョン>
CPU ユニットロギング設定ツール Ver. 1.94Y 以前
CW Configurator Ver. 1.010L 以前
EM Software Development Kit (EM Configurator) Ver. 1.010L 以前
GT Designer3(GOT2000) Ver. 1.221F 以前
GX LogViewer Ver. 1.96A 以前
GX Works2 Ver. 1.586L 以前
GX Works3 Ver. 1.058L 以前
M_CommDTM-HART Ver. 1.00A
M_CommDTM-IO-Link Ver. 1.02C 以前
MELFA-Works Ver. 4.3 以前
MELSEC-L フレキシブル高速 I/O 制御ユニット設定ツール Ver.1.004E 以前
MELSOFT FieldDeviceConfigurator Ver. 1.03D 以前
MELSOFT iQ AppPortal Ver. 1.11M 以前
MELSOFT Navigator Ver. 2.58L 以前
MI Configurator Ver. 1.003D 以前
モーション制御設定 Ver. 1.005F 以前
MR Configurator2 Ver. 1.72A 以前
MT Works2 Ver. 1.156N 以前
RT ToolBox2 Ver. 3.72A 以前
RT ToolBox3 Ver. 1.50C 以前

<バージョンの確認方法>
各製品のマニュアルまたはヘルプをご参照ください。

■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、XML 処理の不備に起因する次の複数の脆弱性が存在します。

・XML 外部実体参照 (XXE) (CWE-611) - CVE-2020-5602
この脆弱性を悪用された場合、悪意ある第三者の攻撃により、該当のソフトウェア製品が動作しているコンピュータ上のファイルが外部に送信される危険性があります。

・リソースの枯渇 (CWE-400) - CVE-2020-5603
この脆弱性を悪用された場合、悪意ある第三者の攻撃により、該当のソフトウェア製品がサービス拒否(DoS)状態に陥る危険性があります。

■脆弱性がもたらす脅威

攻撃者によって悪意を持って細工されたプロジェクトファイル/設定データファイルをお客様が使用する際に、次のような影響を受ける可能性があります。

・ユーザ権限でアクセス可能な任意のファイルが外部に送信される
・該当のソフトウェア製品がサービス拒否(DoS)状態に陥る

■対策方法

以下サイトより各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

対策バージョンは以下となります。

<製品とバージョン>
CPU ユニットロギング設定ツール Ver. 1.100E 以降
CW Configurator Ver. 1.011M 以降
EM Software Development Kit (EM Configurator) Ver. 1.015R 以降
GT Designer3(GOT2000) Ver. 1.225K 以降
GX LogViewer Ver. 1.100E 以降
GX Works2 Ver. 1.590Q 以降
GX Works3 Ver. 1.060N 以降
M_CommDTM-HART Ver. 1.01B 以降
M_CommDTM-IO-Link Ver. 1.03D 以降
MELFA-Works Ver. 4.4 以降
MELSEC-L フレキシブル高速 I/O 制御ユニット設定ツール Ver.1.005F 以降
MELSOFT FieldDeviceConfigurator Ver. 1.04E 以降
MELSOFT iQ AppPortal Ver. 1.14Q 以降
MELSOFT Navigator Ver. 2.62Q 以降
MI Configurator Ver. 1.004E 以降
モーション制御設定 Ver. 1.006G 以降
MR Configurator2 Ver. 1.100E 以降
MT Works2 Ver. 1.160S 以降
RT ToolBox2 Ver. 3.73B 以降
RT ToolBox3 Ver. 1.60N 以降

<アップデート方法>
各製品のマニュアルまたはヘルプをご参照ください。

■回避策

すぐに製品をアップデート出来ないお客様に対し、これらの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。

- 該当製品で使用するプロジェクトファイルや設定データファイルを、メール、USB メモリ、ファイルサーバなどで第三者から受け取る場合は、ファイルが正しい入手経路で取得されたものであることを確認する。(または、入手経路不明なファイルが混入してないことを確認する。)
- 該当製品を管理者権限を持たないアカウントで操作する。
- 該当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。
- すべての制御システムデバイスやシステムのネットワーク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する。
- 制御システムネットワークとリモートデバイスをファイアウォールで防御し、OA ネットワークから分離する。
- リモートアクセスが必要な場合は、仮想プライベートネットワーク(VPN)を使用する。

■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。