

MELSOFT FieldDeviceConfigurator 製品における 任意のコードが実行される脆弱性

公開日 2021年2月16日
最終更新日 2021年6月17日
三菱電機株式会社

■概要

三菱電機が提供する MELSOFT FieldDeviceConfigurator には、M&M Software 社製の fdtCONTAINER コンポーネントに起因する脆弱性が存在します。本脆弱性を悪用された場合、悪意のあるコードが実行され、情報の漏えい、情報の破壊・改ざん、サービス拒否(DoS)などを引き起こす可能性があります。(CVE-2020-12525)

この問題の影響を受ける MELSOFT FieldDeviceConfigurator のバージョンを以下に示しますので、対策方法、あるいは軽減策に記載の内容を実施してください。

■CVSS スコア

CVE-2020-12525 CVSS 3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H 基本値:7.3

■該当製品の確認方法

影響を受ける製品およびバージョンは以下の通りです。
・MELSOFT FieldDeviceConfigurator Ver. 1.05F 以前

<バージョンの確認方法>

1. 当該製品を実行します。
2. メニューの[ヘルプ] → [バージョン情報]を選択します。
3. [バージョン情報]画面が表示されるので、バージョンを確認します。



■脆弱性の説明

三菱電機が提供する MELSOFT FieldDeviceConfigurator には、M&M Software 社製の fdtCONTAINER コンポーネントにおける信頼されていないデータの逆シリアル化(CWE-502)により、任意の不正なコードが実行される脆弱性(CVE-2020-12525)が存在します。

■脆弱性がもたらす脅威

攻撃者により悪意のあるコードを埋め込まれたプロジェクトをお客様が開いた時に、お客様のユーザー権限で悪意のあるコードが実行されることにより、情報の漏えい、情報の破壊、情報の改ざん、サービス拒否(DoS)などを引き起こす可能性があります。

■対策方法

以下サイトより Ver. 1.06G 以降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. 古いバージョンをアンインストールします。
2. ダウンロードしたファイル(zip 形式)を解凍します。
3. 解凍されたフォルダー中にある、「setup.exe」をダブルクリックしてインストールを行ってください。

■軽減策

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。

- ・当該製品で使用する DTM 構成ファイル (*.dtmx) を入手した場合、信頼できる相手から、信頼できる経路にて入手したファイルであることを確認する。
- ・当該製品を管理者権限を持たないアカウントで操作する。
- ・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。

■お客様からのお問い合わせ先

お客様からのお問い合わせ先につきましては、製品をご購入いただいた弊社の支社、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

2021年6月17日

MELSOFT FieldDeviceConfigurator の「該当製品の確認方法」、「対策方法」の情報を追加しました。