複数の三菱電機数値制御装置用ソフトウェアツール及び産業用 IoT 関連製品における Flexera InstallShield に起因する悪意のあるプログラムが実行される脆弱性

公開日 2025 年 7 月 24 日
最終更新日 2025 年 11 月 27 日
三菱電機株式会社

■概要

複数の三菱電機数値制御装置用ソフトウェアツール及び産業用 IoT 関連製品において、Flexera InstallShield に起因する、DLL ハイジャックによる悪意のあるプログラムが実行される脆弱性が存在することが判明しました。攻撃者は、当該製品のインストーラに悪意のある DLL を読み込ませることによって、悪意のあるプログラムを実行することができる可能性があります。(CVE-2016-2542)

なお、本脆弱性は、インストーラの実行時のみに影響を受けるもので、インストール後に影響を与えるものではありません。

■CVSS スコア [1]

CVE-2016-2542　CVSS:v3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H　基本値:7.0

■該当製品の確認方法

影響を受ける製品とバージョンは以下のとおりです。

製品名	バージョン
NC Designer2	全バージョン
NC Designer	全バージョン
NC Configurator2	全バージョン
NC Analyzer2	全バージョン
NC Analyzer	全バージョン
NC Explorer	全バージョン
NC Monitor2	全バージョン
NC Monitor	全バージョン
NC Trainer2 / NC Trainer2 plus	AB 版以前
NC Trainer / NC Trainer plus	全バージョン
NC Visualizer	全バージョン
Remote Monitor Tool	全バージョン
MS Configurator	全バージョン
三菱電機数値制御装置通信用ソフトウェア(FCSB1224)	A8 版以前
三菱 CNC 通信用ランタイムライブラリ M70LC/M730LC	全バージョン
NC Virtual Simulator	全バージョン

<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。以下のサイトから、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

複数の三菱電機数値制御装置用ソフトウェアツール及び産業用 IoT 関連製品には、Flexera Software 社製 InstallShield に起因するファイル検索パスの制御不備(CWE-427[2])により、DLL ハイジャックによる悪意のあるプログラムが実行される脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は、当該製品のインストーラに悪意のある DLL を読み込ませることによって、悪意のあるプログラムを実行することができる可能性があります。

■対策方法

<「■製品での対応」に対策済みバージョンの記載がある製品をご使用中のお客様>

以下のサイトからアップデート版をダウンロードして、インストールを行ってください。

https://www.mitsubishielectric.co.jp/fa/download/index.html

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

2 https://cwe.mitre.org/data/definitions/427.html

<「■製品での対応」に対策済みバージョンの記載がない製品をご使用中のお客様>
軽減策・回避策にて対応をお願いいたします。

なお、以下の製品に対しては、対策版のリリース予定はございません。
NC Designer
NC Analyzer
NC Monitor
NC Trainer / NC Trainer plus
NC Visualizer
Remote Monitor Tool
MS Configurator

■製品での対応
下記製品において、本脆弱性への対策を行っています。

製品名	バージョン
NC Trainer2 / NC Trainer2 plus	AC 版以降
三菱電機数値制御装置通信用ソフトウェア(FCSB1224)	A9 版以降

■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。
・当該製品を使用するパソコンへの物理的なアクセスを制限する。
・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。
・信頼できないファイルを開いたり、信頼できないリンクをクリックしない。
・当社の支社、代理店または三菱電機 FA サイト以外から入手したセットアップランチャを実行しない。
・対象製品のセットアップランチャ実行ファイル(製品により名称は異なります)が格納されているフォルダに、DLL が配置されていないことを確認の上、セットアップランチャを実行する。

■謝辞
この問題をご報告いただいた Sahil Shah 氏に感謝いたします。

■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。

<お問い合わせ窓口一覧(加工機・数値制御装置)| 三菱電機 FA>
https://www.mitsubishielectric.co.jp/fa/about-us/local-network/office20.html

■更新履歴
2025 年 11 月 27 日
対策済みの製品を記載しました。
三菱電機数値制御装置通信用ソフトウェア(FCSB1224)