複数の FA エンジニアリングソフトウェア製品における Jungo 社製 WinDriver に起因する複数の脆弱性

公開日 2024 年 5 月 14 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、Jungo 社製 WinDriver 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。当該ソフトウェア製品がインストールされているコンピュータ上で、悪意のある攻撃プログラムが実行され、これらの脆弱性が悪用された場合に、Windows のブルースクリーン（BSOD）エラーが引き起こされてサービス停止状態(DoS)に陥る危険性及び/又は Windows のシステム権限を取得されることで任意のコマンドが実行される危険性があります（CVE-2023-51776, CVE-2023-51777, CVE-2023-51778, CVE-2024-22102, CVE-2024-22103, CVE-2024-22104, CVE-2024-22105, CVE-2024-22106, CVE-2024-25086, CVE-2024-25087, CVE-2024-25088, CVE-2024-26314）。ただし、これらの脆弱性への攻撃は、Microsoft Windows Defender によって検知されます。

■CVSS スコア [1]

CVE-2023-51776	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N	基本値:4.4
CVE-2023-51777	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	基本値:4.4
CVE-2023-51778	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	基本値:4.4
CVE-2024-22102	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	基本値:4.4
CVE-2024-22103	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	基本値:4.4
CVE-2024-22104	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	基本値:4.4
CVE-2024-22105	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	基本値:4.4
CVE-2024-22106	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:H	基本値:6.0
CVE-2024-25086	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N	基本値:4.4
CVE-2024-25087	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	基本値:4.4
CVE-2024-25088	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N	基本値:4.4
CVE-2024-26314	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N	基本値:4.4

■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。

製品名	バージョン
CPU ユニットロギング設定ツール	全バージョン
CSGL（GX Works2 接続設定画面）	全バージョン
CW Configurator	全バージョン
C 言語コントローラ設定・モニタツール(SW4PVC-CCPU)	全バージョン
EZSocket (*1)	全バージョン
FR Configurator SW3	全バージョン
FR Configurator2	全バージョン
GENESIS64	全バージョン
GT Designer3 Version1 (GOT1000)	全バージョン
GT Designer3 Version1 (GOT2000)	全バージョン
GT SoftGOT1000 Version3	全バージョン
GT SoftGOT2000 Version1	全バージョン
GX Developer	全バージョン
GX LogViewer	全バージョン
GX Works2	全バージョン
GX Works3	全バージョン
iQ Works (MELSOFT Navigator)	全バージョン
MI Configurator	全バージョン
MR Configurator (SETUP221)	全バージョン
MR Configurator2	全バージョン
MRZJW3-MC2-UTL	全バージョン
MX Component	全バージョン
MX OPC Server DA/UA (MC Works64 同梱ソフトウェア)	全バージョン
PX Developer/モニタツール	全バージョン
RT ToolBox3	全バージョン
RT VisualBox	全バージョン
SW0DNC-MNETH-B	全バージョン

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

SW1DNC-CCBD2-B	全バージョン
SW1DNC-CCIEF-J/-B	全バージョン
SW1DNC-MNETG-B	全バージョン
SW1DNC-QSCCF-B	全バージョン
SW1DND-EMSDK-B	全バージョン
データ転送ツール	全バージョン
データ転送ツール Classic	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)	全バージョン

(*1) EZSocket は三菱電機パートナー企業向けの通信ミドルウェア製品です。

<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、Jungo 社製 WinDriver に起因する以下の脆弱性が存在します。
ただし、これらの脆弱性への攻撃は、Microsoft Windows Defender によって検知されます。

CVE ID	脆弱性の説明
CVE-2023-51776	不適切な権限管理(CWE-269[2])による権限昇格の脆弱性
CVE-2023-51777	リソースの枯渇(CWE-400[3])によるサービス拒否(DoS)の脆弱性
CVE-2023-51778	境界外書き込み(CWE-787[4])によるサービス拒否(DoS)の脆弱性
CVE-2024-22102	リソースの枯渇(CWE-400)によるサービス拒否(DoS)の脆弱性
CVE-2024-22103	境界外書き込み(CWE-787)によるサービス拒否(DoS)の脆弱性
CVE-2024-22104	境界外書き込み(CWE-787)によるサービス拒否(DoS)の脆弱性
CVE-2024-22105	リソースの枯渇(CWE-400)よるサービス拒否(DoS)の脆弱性
CVE-2024-22106	不適切な権限管理(CWE-269)による権限昇格及びサービス拒否(DoS)の脆弱性
CVE-2024-25086	不適切な権限管理(CWE-269)による権限昇格の脆弱性
CVE-2024-25087	リソースの枯渇(CWE-400)によるサービス拒否(DoS)の脆弱性
CVE-2024-25088	不適切な権限管理(CWE-269)による権限昇格の脆弱性
CVE-2024-26314	不適切な権限管理(CWE-269)による権限昇格の脆弱性

■脆弱性がもたらす脅威
【CVE-2023-51777, CVE-2023-51778, CVE-2024-22102, CVE-2024-22103, CVE-2024-22104, CVE-2024-22105, CVE-2024-25087】
当該ソフトウェア製品がインストールされているコンピュータ上で、悪意のあるプログラムが実行されることにより、Windows のブルースクリーン(BSOD)エラーが引き起こされてサービス停止状態(DoS)状態に陥る危険性があります。

【CVE-2023-51776, CVE-2024-25086, CVE-2024-25088, CVE-2024-26314】
当該ソフトウェア製品がインストールされているコンピュータ上で、悪意のあるプログラムが実行されることにより、Windows のシステム権限を取得されて任意のコマンドが実行される危険性があります。

【CVE-2024-22106】
当該ソフトウェア製品がインストールされているコンピュータ上で、悪意のあるプログラムが実行されることにより、Windows のブルースクリーン(BSOD)エラーが引き起こされてサービス停止状態(DoS)状態に陥る危険性及び Windows のシステム権限を取得されて任意のコマンドが実行される危険性があります。

■お客様での対応
該当製品をご使用のお客様は、軽減策・回避策にて対応ください。

■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。

■謝辞
これら脆弱性をご報告いただいた today-0day, BoB 12th の Jongseong Kim 様, Byunghyun Kang 様, Sangjun Park 様, Yunjin Park 様, Kwon Yul 様, Seungchan Kim 様に感謝いたします。

2 https://cwe.mitre.org/data/definitions/269.html
3 https://cwe.mitre.org/data/definitions/400.html
4 https://cwe.mitre.org/data/definitions/787.html

■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