

複数の FA 製品における OpenSSL に起因するサービス拒否(DoS)の脆弱性及び 悪意のあるコマンドが実行される脆弱性

公開日 2022 年 8 月 2 日
最終更新日 2023 年 1 月 31 日
三菱電機株式会社

■概要

三菱電機製の複数の FA 製品に搭載している OpenSSL にサービス拒否(DoS)の脆弱性及び悪意のあるコマンド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、細工したパケットを送信することにより、当該製品をサービス停止(DoS)状態に陥らせたり、悪意のあるコマンドを実行することができます。(CVE-2022-0778、CVE-2022-1292)

■CVSS スコア

CVE-2022-0778 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5
CVE-2022-1292 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8

■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。

No	製品名	形名	該当ソフトウェア/ファームウェアバージョン	該当 CVE 番号
1	GOT2000 対応 HMI ソフトウェア	GT SoftGOT2000	1.275M	CVE-2022-0778 CVE-2022-1292
2	CC-Link IE TSN 対応産業用マ ネージドスイッチ	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	03 以前	CVE-2022-0778
3	MELSEC iQ-R シリーズ OPC UA サーバユニット	RD81OPC96	08 以前	CVE-2022-0778

【バージョン確認方法】

- GOT2000 対応 HMI ソフトウェア (形名:GT SoftGOT2000)
 - GT SoftGOT2000 を実行します。
 - メニューの[ヘルプ] -> [バージョン情報]を選択します。
 - [バージョン情報]画面が表示されますので、バージョンを確認します(図 1 参照)。



図 1 GT SoftGOT2000 バージョン情報画面

2. CC-Link IE TSN 対応産業用マネージドスイッチ（形名：NZ2MHG-TSNT8F2、NZ2MHG-TSNT4）

- (1) Web インタフェースで NZ2MHG-TSNT8F2、NZ2MHG-TSNT4 にログイン後、[Device Summary]画面が表示されます。
- (2) [Device Summary]画面に表示される Model Information の Firmware Version に表示される文字の先頭 2 桁の数字を確認します(図 2 参照)。
例)表示される文字が“02 Build xxxx”の場合、ファームウェアバージョンは 02 になります。



図 2 NZ2MHG-TSNT8F2 Model Information 画面

3. MELSEC iQ-R シリーズ OPC UA サーバユニット（形名：RD81OPC96）

- (1) エンジニアリングツール(GX Works3、CW Configurator)を実行し、シーケンサに接続します。
- (2) [診断] -> [システムモニタ] -> [製品情報一覧]ボタンを選択します。
- (3) [製品情報一覧]画面が表示されますので、ファームウェアバージョンを確認します(図 3 参照)。

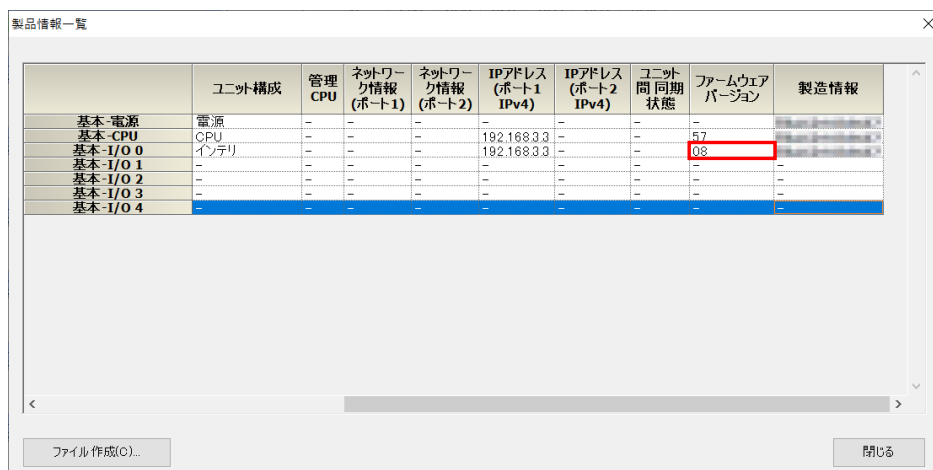


図 3 エンジニアリングツール 製品情報一覧 画面

■脆弱性の説明

三菱電機製の複数の FA 製品に搭載している OpenSSL には、以下の欠陥を起因とするサービス拒否(DoS)の脆弱性(CVE-2022-0778)及び悪意のあるコマンドが実行される脆弱性(CVE-2022-1292)が存在します。

- ・CVE-2022-0778: 無限ループ(CWE-835)
- ・CVE-2022-1292: OS コマンドインジェクション(CWE-78)

■脆弱性がもたらす脅威

攻撃者は、細工したパケットを送信することにより、当該製品をサービス停止(DoS)状態に陥らせたり、悪意のあるコマンドを実行することができます。

■対策方法

該当製品/バージョンをご使用のお客様は、以下に示す手順に従って対策バージョンに更新してください。

【対策バージョン】

No.	製品名	形名	該当ソフトウェア/ファームウェアの対策バージョン
1	GOT2000 対応 HMI ソフトウェア	GT SoftGOT2000	1.280S 以降
2	CC-Link IE TSN 対応産業用マネージドスイッチ	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	04 以降
3	MELSEC iQ-R シリーズ OPC UA サーバユニット	RD81OPC96	09 以降

【更新手順】

1. GOT2000 対応 HMI ソフトウェア (形名:GT SoftGOT2000)

- (1) 三菱電機 FA サイト(<https://www.mitsubishielectric.co.jp/fa/>)のソフトウェアダウンロードコーナーより、最新の GT SoftGOT2000 Version1 をダウンロードし、インストーラのメッセージに従いパソコンにインストールしてください。詳細なインストール手順については「GT SoftGOT2000 Version1 操作マニュアル(SH-081193)」を参照ください。
- (2) 前述のバージョン確認方法に従い、対策バージョンとなっていることを確認してください。

2. CC-Link IE TSN 対応産業用マネージドスイッチ (形名:NZ2MHG-TSNT8F2、NZ2MHG-TSNT4)

- (1) 三菱電機 FA サイト(<https://www.mitsubishielectric.co.jp/fa/>)のダウンロードコーナー(*1)より、CC-Link IE TSN 対応産業用マネージドスイッチの最新のファームウェアファイルをダウンロードしてください。
*1) ダウンロード>ソフトウェア>制御機器>ネットワーク関連製品>ファームウェア>CC-Link IE TSN・アップデート版>産業用スイッチング HUB を選択します。
- (2) Web インタフェースで NZ2MHG-TSNT8F2、NZ2MHG-TSNT4 にログイン後、機能メニューのシステム管理[System Management]のファームウェアアップグレード機能[Firmware Upgrade]を用いて、上記(1)でダウンロードしたファームウェアファイルを選択してファームウェアをアップデートしてください。ファームウェアアップグレードの詳細手順については「CC-Link IE TSN 対応産業用マネージドスイッチ ユーザーズマニュアル(SH-082448)」を参照ください。
- (3) 前述のバージョン確認方法に従い、対策バージョンとなっていることを確認してください。

3. MELSEC iQ-R シリーズ OPC UA サーバユニット (形名:RD81OPC96)

- (1) 三菱電機 FA サイト(<https://www.mitsubishielectric.co.jp/fa/>)のダウンロードコーナー(*2)より、OPC UA サーバユニットの最新のファームウェアファイルをダウンロードしてください。
*2) ダウンロード>ソフトウェア>制御機器>MELSEC iQ-R シリーズ>ファームウェア>情報/ネットワーク・アップデート版>OPC UA サーバユニット を選択します。
- (2) SD メモリカードを使用して、OPC UA サーバユニットのファームウェアをアップデートしてください。ファームウェアアップグレードの詳細手順については「MELSEC iQ-R ユニット構成マニュアル(SH-081222)」を参照ください。
- (3) 前述のバージョン確認方法に従い、対策バージョンとなっていることを確認してください。

■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。

- ・当該製品をインターネットに接続する場合には、仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止してください。
- ・当該製品を LAN 内で使用し、信頼できないネットワークやホストとの通信をファイアウォールでブロックしてください。
- ・当該製品を使用するパソコンおよび同一ネットワーク機器への物理的なアクセスを制限してください。

加えて、対象製品に応じて以下に示す軽減策を講じることを推奨します。

1. GOT2000 対応 HMI ソフトウェア (形名:GT SoftGOT2000)

- ・OPC UA サーバを最新版にアップデートしてご使用ください。
- ・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してください。

2. CC-Link IE TSN 対応産業用マネージドスイッチ (形名:NZ2MHG-TSNT8F2、NZ2MHG-TSNT4)

- ・Web インタフェースで NZ2MHG-TSNT8F2、NZ2MHG-TSNT4 にログイン後、機能メニューのアカウント管理[Account Management]でユーザ名、パスワードをデフォルトから変更してください。また利用者に応じて適切なアクセス権限を設定してください。

3. MELSEC iQ-R シリーズ OPC UA サーバユニット (形名:RD81OPC96)

- ・OPC UA クライアントを最新版にアップデートしてご使用ください。
- ・OPC UA クライアント側で正規の証明書(細工されていないと判断可能な証明書)をご使用ください。

■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 1 月 31 日

「対策方法」のダウンロード手順を修正しました。(三菱電機 FA サイトのレイアウト変更によるもの。)

NZ2MHG-TSNT8F2、NZ2MHG-TSNT4

「対策方法」に対象製品の対策バージョン、更新手順を追加しました。

RD81OPC96

2022 年 11 月 1 日

「対策方法」に対象製品の対策バージョン、更新手順を追加しました。

NZ2MHG-TSNT8F2、NZ2MHG-TSNT4

2022 年 8 月 30 日

「該当製品の確認方法」、「対策方法」、「軽減策・回避策」に下記対象製品を追加しました。

NZ2MHG-TSNT4

2022 年 8 月 18 日

「該当製品の確認方法」に対象製品を追加しました。

「対策方法」に対象製品を追加しました。

「軽減策・回避策」に対象製品の軽減策を追加しました。

NZ2MHG-TSNT8F2、RD81OPC96