CC-Link IE TSN 対応産業用マネージドスイッチ製品における OpenSSL に起因するサービス拒否(DoS)の脆弱性

公開日 2024 年 6 月 4 日
三菱電機株式会社

■概要

CC-Link IE TSN 対応産業用マネージドスイッチ製品に搭載している OpenSSL において、サービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、悪意のある証明書データをインポートさせることにより、処理時間を遅延させ、当該製品の Web サービスを一時的にサービス停止(DoS)状態に陥らせることができる可能性があります。ただし、証明書データのインポートには、管理者権限が必要です。(CVE-2023-2650)

■CVSS スコア [1]

CVE-2023-2650　CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L　基本値:2.7

■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	該当ファームウェアバージョン
1	CC-Link IE TSN 対応産業用マネージドスイッチ	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	05 以前

【バージョン確認方法】

(1) NZ2MHG-TSNT8F2 又は NZ2MHG-TSNT4 の Web インタフェースからログインすると、[Device Summary]画面が表示されます。

(2) [Device Summary]画面で、Model Information の Firmware Version に記載された文字列の先頭 2 文字(数字)を確認します(図 1 参照)。

例) 表示される文字列が"02 Build xxxx"の場合には、ファームウェアバージョンは 02 になります。

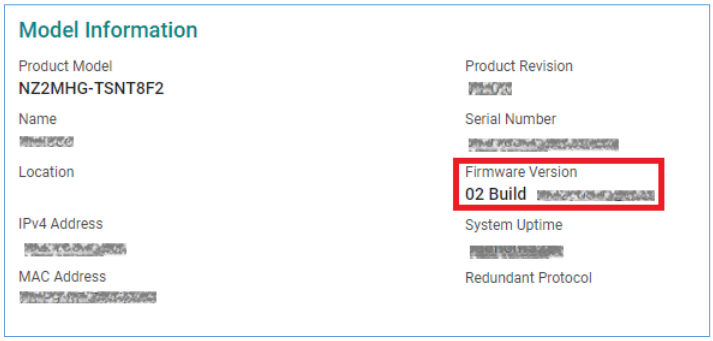

図 1 NZ2MHG-TSNT8F2 Model Information 画面

■脆弱性の説明

CC-Link IE TSN 対応産業用マネージドスイッチに搭載している OpenSSL には、制限またはスロットリング無しのリソースの割り当て(CWE-770[2])に起因する、サービス拒否(DoS)の脆弱性(CVE-2023-2650)が存在します。

■脆弱性がもたらす脅威

攻撃者は、悪意のある証明書データをインポートさせることにより、処理時間を遅延させ、当該製品の Web サービスを一時的にサービス停止(DoS)状態に陥らせることができる可能性があります。ただし、証明書データのインポートには管理者権限が必要です。

[1] https://www.ipa.go.jp/security/vuln/CVSSv3.html
[2] https://cwe.mitre.org/data/definitions/770.html

■対策方法

該当製品をご使用のお客様は、以下に示す手順に従って、ファームウェアを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	該当ファームウェアの対策バージョン
1	CC-Link IE TSN 対応産業用 マネージドスイッチ	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	06 以降

【更新手順】

(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)から、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) NZ2MHG-TSNT8F2 又は NZ2MHG-TSNT4 の Web インタフェースからのログイン後に、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、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デート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。

■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。

・当該製品並びに当該製品と同一のネットワーク内に配置されたパソコンおよび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。

・CC-Link IE TSN 対応産業用マネージドスイッチ（NZ2MHG-TSNT8F2 又は NZ2MHG-TSNT4）の Web インタフェースから NZ2MHG-TSNT8F2 又は NZ2MHG-TSNT4 にログイン後に、機能メニューのアカウント管理[Account Management]でユーザ名及びパスワードを、デフォルト値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。

■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