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 に起因する情報漏えいの脆弱性 及びサービス拒否(DoS)の脆弱性

公開日 2023 年 10 月 5 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、情報漏えいの脆弱性及びサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、細工したパケットを送信することにより当該製品に登録している情報を入手したり、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当該製品をサービス停止(DoS)状態に陥らせることができる可能性があります。(CVE-2022-4304、CVE-2022-4450)

■CVSS スコア [1]

CVE-2022-4304　CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N　基本値:5.9
CVE-2022-4450　CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H　基本値:6.5

■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	全バージョン

■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、以下 2 件の脆弱性が存在します。

・CVE-2022-4304:RSA での復号の実装に存在するタイミングの違いに起因する情報漏えい(CWE-208[2])による、情報漏えいの脆弱性
・CVE-2022-4450:PEM 形式のデータの読み込み時の二重解放(CWE-415[3])による、サービス拒否(DoS)の脆弱性

■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し、Bleichenbacher 攻撃(*1)を行うことにより、暗号文を解読し、機微な情報を窃取できる可能性があります(CVE-2022-4304)。また、攻撃者は、悪意のある証明書をインポートすることにより、当該製品をサービス停止(DoS)状態に陥らせることができる可能性があります(CVE-2022-4450)。

*1:パディングエラーが発生した際の実行時間の違いを観察することにより、暗号文の解読を行う攻撃

■対策方法

軽減策・回避策にて対応をお願いいたします。

■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、NZ2MHG-TSNT4)の 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。

■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

[1] https://www.ipa.go.jp/security/vuln/CVSSv3.html
[2] https://cwe.mitre.org/data/definitions/208.html
[3] https://cwe.mitre.org/data/definitions/415.html