MELSOFT MaiLab 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 7 月 18 日
三菱電機株式会社

■概要
MELSOFT MaiLab 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、細工したメッセージ認証コードを送信することにより、対象をサービス停止(DoS)状態に陥らせることができる可能性があります。(CVE-2023-4807)

■CVSS スコア [1]
CVE-2023-4807 CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値: 5.9

■該当製品の確認方法
影響を受ける製品は以下のとおりです。

No	製品名	形名	該当ソフトウェアバージョン
1	MELSOFT MaiLab	SW1DND-MAILAB-M SW1DND-MAILABPR-M	ver.1.00A～1.05F

【バージョンの確認方法】
(1) MELSOFT MaiLab を起動します。
(2) 開いた設定管理ツールに記載されたバージョン情報を確認します(図 1 参照)。

図 1 MELSOFT MaiLab 画面

■脆弱性の説明
MELSOFT MaiLab で使用している OpenSSL ライブラリには、POLY1305 メッセージ認証コード(MAC)の実装の不具合により、デジタル署名の不適切な検証(CWE-347)[2]に起因するサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威
攻撃者が、TLS 通信時に POLY1305 による認証付き暗号を使用するモードを選択し、細工したメッセージ認証コードを送信することによりサービス停止(DoS)状態に陥る可能性があります。

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/347.html

■対策方法

下記のサイトから、下表に記載の対策済みバージョンをダウンロードし、アップデートしてください。

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

No	製品名	形名	ソフトウェアバージョン
1	MELSOFT MaiLab	SW1DND-MAILAB-M SW1DND-MAILABPR-M	ver.1.06G 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に、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、ファイアウォールや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。

・当該製品を制御システム内で使用し、制御システム内のネットワークとデバイスをファイアウォールで防御することによって、信頼できないネットワークやホストからのアクセスを遮断してください。

・当該製品がインストールされた PC および PC が接続されているネットワークへの物理的なアクセスを制限し、不正な接触を防止してください。

・信頼できない送信元からのメール等に記載された Web リンクをクリックしないようにします。また信頼できない電子メールの添付ファイルを開かないようにしてください。

■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