公開日　2022 年 09 月 01 日
株式会社コンテック

FLEXLAN FX3000 および FX2000 シリーズの脆弱性と対策について

■ 概要

当社の無線 LAN 製品 FLEXLAN FX3000 および FX2000 シリーズにおいて、ファームウェアに脆弱性が存在することが判明しました。本脆弱性を悪意ある攻撃者に悪用された場合、データの盗用や改竄、悪意のあるプログラムを実行しシステムを破壊される等の可能性があります。
この問題の影響を受ける製品ならびにファームウェアのバージョンを以下に記し、脆弱性の概要ならびに対策方法・回避策を説明します。

■ 該当製品

シリーズ名	FLEXLAN FX3000 シリーズ		FLEXLAN FX2000 シリーズ
型式	FXA3200 FXA3000 FXA3000-US FXA3000-EU FXA3000-TW FXA3000-KR FXA3020	FXE3000 FXE3000-US FXE3000-EU FXE3000-TW FXE3000-KR FXE3000-WP FXS3000-CN FXS3001-CN	FXA2000 FXA2000-G FXA2020 FXA2300 FXE2000 FXE2000-G FXR2000 FXR2000-G
ファームウェア バージョン	Ver.1.16.00 未満		Ver.1.39.00 未満

■ 判明した脆弱性と脆弱性がもたらす脅威

上記の該当ファームウェアバージョンの該当製品は、Web 設定画面にどこからもリンクされていない開発者用のシステムコマンドを実行できる非公開の画面を用意しています。Web 設定画面に接続することができる（パスワードを知っている）悪意あるユーザにこの画面を利用されることで、データの盗用や改竄、システムの破壊、悪意のあるプログラムの実行等が行われる可能性があります。

■ 対策方法

ファームウェアを最新版に更新してください。FX3000 シリーズは Ver.1.16.00 以降、FX2000 シリーズは Ver.1.39.00 以降になります。
最新のファームウェアは当社 Web サイトより入手できます。型式を入力してファームウェアを指定して検索してください。
https://www.contec.com/jp/download/search/
対策ファームウェアは下記のソフトウェア更新情報からも入手できます。
https://www.contec.com/jp/software-update/2022/22082900/
ファームウェアの更新手順につきましては解説書、または Web 設定画面のヘルプをご確認ください。

■ 回避策

対策バージョンに更新できないお客様に対し、これらの脆弱性が悪用されるリスクを最小限に抑えるために、当社は以下に示す軽減策を講じることを推奨します。

- 本製品の Web 設定画面に接続するためのパスワードをデフォルトから変更する
- 本製品のネットワークに不正アクセスされないようにファイアウォール等を設置する

■ 関連情報

JVNVU#98305100 Contec製FLEXLAN FX3000およびFX2000シリーズにおける複数の脆弱性

■ 謝辞

本脆弱性の発見者である Thomas Knudsen 氏、Samy Younsi 氏に厚く御礼申し上げます。

■ お問合せ先

テクニカルサポートセンター　https://www.contec.com/jp/support/technical-support/