

SolarView Compact (SV-CPT-MC310)の脆弱性について

■概要

当社製の太陽光発電計測監視装置「SolarView Compact」において複数の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影響を受ける恐れがあります。

この問題の影響を受ける製品ならびに対策方法・回避策を以下に示しますので、対策または軽減策・回避策の実施をお願いいたします。

■該当製品

製品名 : SolarView Compact
型式 : [SV-CPT-MC310](#)、[SV-CPT-MC310F](#)
バージョン : Ver.6.50 未満

<バージョンの確認方法>

製品に Web ブラウザでアクセスし、メニューから「設定」→「オプション」→「システム更新」を開き、「名称[バージョン]」にて確認できます。

■判明した脆弱性と脆弱性がもたらす脅威

[【JVN#37417423】](#)

①「SolarView Compact における OS コマンドインジェクションの脆弱性」

ネットワーク導通確認画面から OS が実行できるコマンドを入力することができ、悪意ある攻撃者に利用されることで情報の盗用・改竄、システムの破壊、悪意あるプログラムの実行等が行われる可能性があります。

②「SolarView Compact における任意のファイルアップロードの脆弱性」

画像管理やシステム更新画面より任意のファイルがアップデートできる仕様となっており、悪意ある攻撃者に利用されることでマルウェア等の不正なソフトウェアをアップロードされる可能性があります。

③「SolarView Compact における使用製品の既知の脆弱性」

Web サーバ、FTP サーバが既知の脆弱性が報告されているバージョンとなっており、悪意ある攻撃者に脆弱性を利用されることで情報の改竄、サービスの停止、システムの破壊を実行される可能性があります。

④「SolarView Compact におけるディレクトリリスティングの脆弱性」

Web サーバの設定に不適切な点があり特定ディレクトリのファイル一覧が取得でき、悪意ある攻撃者に利用されることで情報を盗用される可能性があります。

⑤「SolarView Compact におけるクロスサイトスクリプティングの脆弱性」

Web アプリケーションに POST、GET されるデータのサニタイズ処理に問題があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導が行われる可能性があります。

⑥「SolarView Compact におけるディレクトリトラバーサル脆弱性」

画像管理画面にて URL から直接パラメータを渡すことで画像以外のファイルが削除でき、悪意のある攻撃者に利用されることでシステムが破壊される可能性があります。

⑦「SolarView Compact におけるアクセス制限不備脆弱性」

認証が必要となる画面に対し、URL を直接入力することで認証を回避できてしまい、悪意ある攻撃者に利用されることで設定情報の盗用・改竄が行われる可能性があります。

⑧「SolarView Compact におけるアクセス制限不備脆弱性」

Web アプリケーションの中に任意のファイルの編集を行えるテキストエディタが含まれており、悪意ある攻撃者に利用されることで情報の改竄、悪意あるプログラムの作成が行われる可能性があります。

【その他 ([JVN#37417423](#)対象外)】

⑨「SolarView Compact における認証不備脆弱性」

システム内部の管理者権限のパスワードが推測可能なものとなっており、悪意のある攻撃者に管理者権限を取得される可能性があります。

■対策方法

ソフトウェア（ドライバ）を最新版（Ver.6.50 以降）に更新してください。

最新のソフトウェアは当社 Web サイトより入手できます。

- ・ [最新ソフトウェア \(SolarView Compact ファームウェア アップデータ\)](#)
- ・ [SolarViewシリーズ ファームウェア アップデート手順書](#)

■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。

- ・ 本製品をネットワーク回線から切り離す
- ・ 本製品のネットワークの上流側にファイアウォールを設置する
- ・ 本製品のネットワークアクセスを信頼できる閉域網で構成する
- ・ 本製品の「ユーザー設定」にて「ユーザー認証範囲の設定」を「全画面を認証対象にする」で設定する

■お問い合わせ先

ソリューションサポートセンター

TEL : 050-3786-4985/03-6625-5541 E-mail : ssc@jp.contec.com

■更新履歴

2021 年 2 月 24 日

「SolarView Compact における認証不備脆弱性」を JVN#37417423 対象から除外

2021 年 2 月 17 日

各脆弱性の脆弱性識別番号を削除