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 : 8.10 未満

<バージョンの確認方法>

Webブラウザで製品にアクセスし、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

【JVNVU#92106300】

- ① CVE-2023-27512 : 「SolarView Compact におけるハードコードされた認証情報の使用」… CWE-798

非公開の管理者用アカウントの認証情報がハードコーディングされており、悪意ある攻撃者が認証情報を使うことで情報の盗用・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。

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N 基本値 : 6.5

- ② CVE-2023-27514 : 「SolarView Compact における OS コマンドインジェクションの脆弱性」… CWE-78

ダウンロード画面にて HTTP リクエストが適切に検証されないことにより、OS が実行できるコマンドを送信でき、悪意ある攻撃者に利用されることで情報の盗用・改竄、システムの破壊等を行われる可能性があります。

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値 : 8.8

- ③ CVE-2023-27518 : 「SolarView Compact におけるバッファオーバーフローの脆弱性」… CWE-120

複数の設定画面にバッファオーバーフローの脆弱性があり、悪意ある攻撃者に利用されることで情報の盗用・改竄、システムの破壊等を行われる可能性があります。

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L 基本値 : 6.3

-
- ④ CVE-2023-27521:「SolarView Compact における OS コマンドインジェクションの脆弱性」
…CWE-78

※CVE-2022-29303 の修正不十分による脆弱性

メール送信設定画面にて HTTP リクエストが適切に検証されないことにより、OS が実行できるコマンドを送信でき、悪意ある攻撃者に利用されることで情報の盗用・改竄、システムの破壊等を行われる可能性があります。

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値 : 8.8

- ⑤ CVE-2023-27920:「SolarView Compact におけるアクセス制限不備の脆弱性」…CWE-284

システム日時設定画面にてアクセス制限が適切に適用されないことにより、通常ユーザー権限にアクセスでき、悪意ある攻撃者に利用されることでシステム日時の変更や CVE-2023-27518 の脆弱性を利用される可能性があります。

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N 基本値 : 4.3

■ 対策方法

ソフトウェア(ファームウェア)を最新版(Ver.8.10 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

■ 関連情報

- ・ JVN#92106300 「コンテック製 SolarView Compact における複数の脆弱性」
<https://jvn.jp/vu/JVN#92106300/>

■ 謝辞

本脆弱性の発見者である株式会社ゼロゼロワン 早川 宙也 氏に厚く御礼申し上げます。

■ 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

■ 改訂履歴

- ・ 2023 年 05 月 08 日 初版