公開日　2026 年 09 月 10 日

株式会社コンテック

当社 SolarView シリーズ製品における脆弱性について

■概要

複数の当社製品において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・回避策を製品シリーズごとに示します。対策、軽減または回避策の実施をお願いいたします。

対象製品名一覧

① 太陽光発電計測 SolarView シリーズ　SolarView Compact

該当製品①

シリーズ名　：太陽光発電計測SolarViewシリーズ
製品名　　：SolarView Compact
製品型式　　：SV-CPT-MC310
　　SV-CPT-MC310F
バージョン　：9.00 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

① CVE-2026-82794：「SolarView Compact における OS コマンドインジェクション」…CWE-78
スケジュール設定画面にて 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や改竄、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

② CVE-2026-82795：「SolarView Compact におけるクロスサイトスクリプティング」…CWE-79
スケジュール設定、メール送信設定画面にてクロスサイトスクリプティングの脆弱性があり、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を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:L / UI:R / S:C / C:L / I:L / A:N　　基本値：5.4

③ CVE-2026-82796：「SolarView Compact におけるクロスサイトスクリプティング」…CWE-79
画像の登録画面にてクロスサイトスクリプティングの脆弱性があり、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を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:L / UI:R / S:C / C:L / I:L / A:N　　基本値：5.4

・対策方法

ファームウェアを上記脆弱性の対策を施した最新バージョンに更新してください。
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。
ファームウェアの更新手順につきましては、マニュアルやヘルプなどをご確認ください。

- SV-CPT-MC310 / 310F（対策済みバージョン：Ver. 9.0 以降）
  https://www.contec.com/jp/download/contract/contract-none/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e&downloaditemid=af776a2c-9270-4362-8b17-9811260c990d

ダウンロード検索を使用する場合は、以下の検索サイトにアクセスの上、対象製品の型式を入力し、ファームウェアを指定して検索してください。

- 検索サイト
  https://www.contec.com/jp/download/search/

・回避策

対策済み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し信頼できる通信のみ許可する
・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

■関連情報

・JVNVU#97753461
https://jvn.jp/vu/JVNVU97753461/

■お問い合わせ先

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

■改訂履歴

・2026 年 09 月 10 日　　初版