公開日　2026 年 11 月 06 日

株式会社コンテック

SolarView シリーズ製品における PHP の脆弱性について

■ 概要

The PHP Group から、PHP における 2 件の脆弱性（CVE-2026-109618、CVE-2026-109619）が公開されました。これらの脆弱性が悪用された場合、認証されていない遠隔の第三者により、対象システム上で任意のコードを実行される可能性があります。
当社で調査した結果、以下の SolarView シリーズ製品が本脆弱性の影響を受けることを確認しました。対象製品と対応方法を以下に示します。

対象製品名一覧

① 太陽光発電計測 SolarView シリーズ　SolarView Compact
② 太陽光発電計測 SolarView シリーズ　SolarView Air※1
③ 太陽光発電計測 SolarView シリーズ　SolarView 遠隔操作ボックス

※1 SolarView Air は閉域網のネットワークで構成された製品の為、本脆弱性がシステムの運用にあたえる影響はありません。

■ **対象製品 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　：9.02 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」→「システム情報」を開き、「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-2026-109618：「PHP のメモリ不足時の処理に起因する脆弱性」…CWE-416
認証されていない遠隔の第三者により、任意のコードを実行される可能性があります。
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
基本値：9.2（The PHP Group の公表）

② CVE-2026-109619：「PHP の解放済みメモリに関連する内部状態の処理に起因する脆弱性」…CWE-416
認証されていない遠隔の第三者により、任意のコードを実行される可能性があります。
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
基本値：9.2（The PHP Group の公表）

● **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 サイトから入手できます。
ファームウェアの更新手順については、マニュアルやヘルプを参照してください。

- SV-CPT-MC310 / MC310F（対策済みバージョン：Ver. 9.02 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、当社は以下に示す回避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

■ **対象製品 ②**

シリーズ名　：太陽光発電計測SolarViewシリーズ
製品名　　：SolarView Air
製品型式　　：SV-AIR-MC310、SV-AIR-MC310-P01
バージョン　：9.02 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」→「システム情報」を開き、「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-2026-109618 :「PHP のメモリ不足時の処理に起因する脆弱性」…CWE-416
認証されていない遠隔の第三者により、任意のコードを実行される可能性があります。
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
基本値：9.2（The PHP Group の公表）

② CVE-2026-109619 :「PHP の解放済みメモリに関連する内部状態の処理に起因する脆弱性」…CWE-416
認証されていない遠隔の第三者により、任意のコードを実行される可能性があります。
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
基本値：9.2（The PHP Group の公表）

※ 本製品はインターネットからアクセスができない閉域網のネットワークで運用されています。その為、システムの運用に脅威を受けることはありません。

● **対策方法**

SV-AIR-MC310 / -P01 については、必要であれば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 サイトから入手できます。
ファームウェアの更新手順については、マニュアルやヘルプを参照してください。

- SV-AIR-MC310 / -P01（対策済みバージョン：Ver. 9.02 以降）
  https://www.contec.com/jp/download/contract/contract-none/?itemid=319f2d16-ff9b-4950-8828-0f2bc8fda75c&downloaditemid=83da32a8-e65e-4c02-973e-e2b6138b96e6
- 本製品が接続する SolarView Air クラウドシステムは当社にて 2026 年 10 月 22 日に対応を実施済みです。お客様による対応は不要です。

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/

■ **対象製品 ③**

シリーズ名　：太陽光発電計測SolarViewシリーズ
製品名　　：SolarView 遠隔操作ボックス
製品型式　　：SV-OPT-RRY2-BOX
バージョン　：2.14 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「メンテナンス」→「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**

③ CVE-2026-109618 :「PHP のメモリ不足時の処理に起因する脆弱性」…CWE-416
認証されていない遠隔の第三者により、任意のコードを実行される可能性があります。
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
基本値：9.2（The PHP Group の公表）

④ CVE-2026-109619 :「PHP の解放済みメモリに関連する内部状態の処理に起因する脆弱性」…CWE-416
認証されていない遠隔の第三者により、任意のコードを実行される可能性があります。
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
基本値：9.2（The PHP Group の公表）

● **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 サイトから入手できます。
ファームウェアの更新手順については、マニュアルやヘルプを参照してください。

- SV-OPT-RRY2-BOX（対策済みバージョン：Ver. 2.14 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=cedb473b-8cbb-42dc-a3e3-da32bfa2c1b1&downloaditemid=0ce45fa9-df53-48c5-8e17-f2168882fe09

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**

- The PHP Group
  https://www.php.net/archive/2026.php#2026-10-21-5
- JVNVU#99905564
  https://jvn.jp/vu/JVNVU99905564/

■ **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/tsc/

■ **改訂履歴**

2026 年 11 月 06 日　初版