公開日　2026 年 11 月 06 日

株式会社コンテック

PC-HELPER 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 PC-HELPER 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 PC HELPER シリーズ　　CAN 通信コンバータ

■ **対象製品 ①**

シリーズ名　：PC-HELPER CAN通信コンバータ
製品名　　：CAN2.0B通信 無線LAN/USBコンバータユニット 2ch
　　：CAN2.0B通信 USBコンバータユニット 2ch
製品型式　　：CAN-2-WF
　　：CAN-2-USB
バージョン　：2.30 未満

<バージョンの確認方法>
機器に Web ブラウザでアクセスすることで画面右上から確認できます。



- **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。
なお、Ver.2.14 以前のファームウェアをご使用の場合は、Ver.2.20 へ更新した後に Ver.2.30 以降へ更新する必要があります。
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 Readme を参照してください。

- CAN-2-WF, CAN-2-USB（対策済みバージョン：Ver.2.30 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=3e5442c9-333c-478a-938a-fdcd5153c058&downloaditemid=9b3fb805-2018-4c73-a644-6b4c209dc329

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

■ **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