公開日　2026 年 09 月 10 日

株式会社コンテック

当社 PC-HELPER 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 PC-HELPER シリーズ	ワイヤレス I/O
② PC-HELPER シリーズ	CAN 通信コンバータ

■該当製品①

シリーズ名　：　PC-HELPER ワイヤレスI/O
製品名　　：　ワイヤレスI/O
製品型式　　：　DIO-0404RY-LWF、DIO-0404RY-LWF-US
バージョン　：　1.01.00 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-2026-82790：「PC-HELPER DIO-0404RY-LWF におけるクロスサイトスクリプティングの脆弱性」…CWE-79
設定画面に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

② CVE-2026-82764：「コンテック製品におけるクロスサイトリクエストフォージェリ」…CWE-352
クロスサイトリクエストフォージェリの脆弱性があり、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:N / UI:R / S:U / C:N / I:L / A:N　　基本値：4.3

・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。

- DIO-0404RY-LWF / -LWF-US（対策済みバージョン：Ver. 1.01.00 以降）
  https://www.contec.com/jp/products-services/daq-control/pc-helper/wireless-io/dio-0404ry-lwf/support/#firmware

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

■該当製品②

シリーズ名　：　PC-HELPER CAN通信コンバータ
製品名　　：　CAN 2.0B通信 無線LAN/USBコンバータユニット
製品型式　　：　CAN-2-WF、CAN-2-USB
バージョン　：　2.20 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-2026-82791：「PC-HELPER CAN 通信コンバータにおける OS コマンドインジェクション」…CWE-78
設定画面に 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-2026-82792：「PC-HELPER CAN 通信コンバータにおけるクロスサイトスクリプティングの脆弱性」…CWE-79
設定画面に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:A / AC:L / PR:N / UI:R / S:C / C:L / I:L / A:N　　基本値：5.2

③ CVE-2026-82793：「PC-HELPER CAN 通信コンバータにおける危険なタイプのファイルの制限なしアップロード」…CWE-434
悪意のある攻撃者によって改竄されたファイルをアップロードすることができ、悪意の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:H / UI:N / S:U / C:H / I:H / A:H　　基本値：7.2

・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。

- CAN-2-WF, CAN-2-USB（対策済みバージョン：Ver. 2.20 以降）
  https://www.contec.com/jp/products-services/daq-control/pc-helper/wireless-io/can-2-wf/support/#firmware

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#90314828
https://jvn.jp/vu/JVNVU90314828/

■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