公開日　2026 年 09 月 10 日

株式会社コンテック

当社 CONPROSYS 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 CONPROSYS M2M シリーズ	CONPROSYS M2M Gateway、M2M コントローラ
② CONPROSYS PAC シリーズ	CONPROSYS PAC
③ CONPROSYS TM シリーズ	CONPROSYS TM
④ CONPROSYS Nano シリーズ	CONPROSYS Nano
⑤ CONPROSYS IO-Link マスタ	CONPROSYS IO-Link マスタ
⑥ CONPROSYS HMI SYSTEM	CONPROSYS HMI SYSTEM(CHS)

対象商品①

シリーズ名	：	CONPROSYS M2Mシリーズ	
製品名	：	CONPROSYS M2M Gateway、M2Mコントローラ	
製品型式	：	M2M Gatewayコンパクトタイプ	CPS-MG341*
		M2M Gatewayスタックタイプ	CPS-MGS341*
		M2Mコントローラコンパクトタイプ	CPS-MC341*
		M2Mコントローラスタックタイプ	CPS-MCS341*
バージョン	：	M2M Gateway コンパクトタイプ	4.1.0 未満
		M2M Gateway スタックタイプ	4.1.0 未満
		M2M コントローラコンパクトタイプ	4.1.0 未満
		M2M コントローラスタックタイプ	4.1.0 未満

・判明した脆弱性と脆弱性がもたらす脅威

① CVE-2026-82773：「CONPROSYS M2M シリーズにおけるクロスサイトスクリプティング」…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:N / UI:R / S:C / C:L / I:L / A:N　　基本値：6.1

② CVE-2026-82774：「CONPROSYS M2M シリーズにおける 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・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-2026-82775：「CONPROSYS M2M シリーズにおけるディレクトリブラウジング」…CWE-548
Web ブラウザから不正な URL を指定することでディレクトリの一覧が取得でき、悪意ある攻撃者に利用されることで情報の盗用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:L / I:N / A:N　　基本値：4.3

④ CVE-2020-7746：「コンテック製品における脆弱な JavaScript ライブラリの使用」…CWE-1395
脆弱性を含む JavaScript ライブラリを使用しており、悪意ある攻撃者に利用されることで情報の盗用、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:N / S:U / C:N / I:N / A:H　　基本値：7.5

・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。

- M2M Gateway コンパクトタイプ（対策済みバージョン：Ver. 4.1.0 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=f832c526-dcf6-4976-85aa-f536c15a8120&downloaditemid=05de36ae-f9da-4027-8638-c82bcf3f6e1a

- M2M Gateway スタックタイプ（対策済みバージョン：Ver. 4.1.0 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=f3e65c0f-8fdc-4104-ae18-22595cfb17ed&downloaditemid=735deb39-86c7-40cd-a422-d40f17859370

- M2M コントローラコンパクトタイプ（対策済みバージョン：Ver. 4.1.0 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=46a296a9e-29ea-46f2-9254-6b3297c6d21b&downloaditemid=d0af32d3-c247-480f-b613-fc17c9e9f980

- M2M コントローラスタックタイプ（対策済みバージョン：Ver. 4.1.0 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=5a6f066f-5a7a-4756-bce8-13e1345e5f7a&downloaditemid=68a45c33-392b-4988-aa18-349cd6a9d8d4

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

対象商品②

シリーズ名	:	CONPROSYS PACシリーズ	
製品名	:	CONPROSYS PAC	
製品型式	:	コンパクトタイプ	CPS-PC341□□-*-9201
		スタックタイプ	CPS-PCS341□□-DS1-1201
バージョン	:	コンパクトタイプ	3.0.0 未満
		スタックタイプ	3.0.0 未満

・判明した脆弱性と脆弱性がもたらす脅威

① CVE-2026-82776：「CONPROSYS PAC シリーズにおけるクロスサイトスクリプティング」…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:N / UI:R / S:C / C:L / I:L / A:N　　基本値：6.1

② CVE-2026-82777：「CONPROSYS PAC シリーズにおける 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・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-2026-82778：「CONPROSYS PAC シリーズにおけるディレクトリブラウジング」…CWE-548
Web ブラウザから不正な URL を指定することでディレクトリの一覧が取得でき、悪意ある攻撃者に利用されることで情報の盗用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:L / I:N / A:N　　基本値：4.3

④ CVE-2020-7746：「コンテック製品における脆弱な JavaScript ライブラリの使用」…CWE-1395
脆弱性を含む JavaScript ライブラリを使用しており、悪意ある攻撃者に利用されることで情報の盗用、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:N / S:U / C:N / I:N / A:H　　基本値：7.5

・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。

- コンパクトタイプ（対策済みバージョン：Ver. 3.0.0 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=c3bc6f62-acca-4276-a586-f74e50ba5b44&downloaditemid=98d39469-764f-4ef9-bf05-2b2e7d684874

- スタックタイプ（対策済みバージョン：Ver. 3.0.0 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=5728762f-64b6-4550-b27e-12588e753e0a&downloaditemid=ce7cb1e2-7b1a-40d7-96a9-cde22bc87c31

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③

シリーズ名　：CONPROSYS TMシリーズ
製品名　　：CONPROSYS TM
製品型式　　：CPS-TM341G5MB-ADSC1-931
CPS-TM341MB-ADSC1-931
CPS-TM341GMB-ADSC1-931
バージョン　：2.19 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、「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-2026-82779：「CONPROSYS TM シリーズにおける OS コマンドインジェクション」…CWE-78
ユーザー設定画面に 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・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-2026-82780：「CONPROSYS TM シリーズにおける危険な任意のファイルのアップロード」…CWE-434
モニタの編集画面に危険な任意のファイルをアップロードできる脆弱性があり、悪意の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-2020-7746：「コンテック製品における脆弱な JavaScript ライブラリの使用」…CWE-1395
脆弱性を含む JavaScript ライブラリを使用しており、悪意ある攻撃者に利用されることで情報の盗用、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:N / S:U / C:N / I:N / A:H　　基本値：7.5

・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。

- CPS-TM341MB/GMB/G5MB（対策済みバージョン：Ver. 2.19 以降）
https://www.contec.com/jp/download/contract/contract2/?itemid=349f41d1-4b3a-438b-a71d-5f857e8f18e0&downloaditemid=ad140091-6cdb-49c6-9322-fe646042b614

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

対象商品④

シリーズ名	：	CONPROSYS Nanoシリーズ	
製品名	：	リモートI/Oカプラユニット(サーバタイプ)	
		リモートI/Oカプラユニット(EtherNet/IPアダプタ)	
		プログラマブルリモートI/Oカプラユニット(ソフトPLCタイプ)	
製品型式	：	リモートI/Oカプラユニット(サーバタイプ)	CPSN-MCB271-*
		リモートI/Oカプラユニット(EtherNet/IPアダプタ)	CPSN-EOB471EI-□1
		プログラマブルリモートI/Oカプラユニット(ソフトPLCタイプ)	CPSN-PCB271-S1-041
バージョン	：	リモートI/Oカプラユニット(サーバタイプ)	1.82未満
		リモートI/Oカプラユニット(EtherNet/IPアダプタ)	1.02未満
		プログラマブルリモートI/Oカプラユニット(ソフトPLCタイプ)	1.61未満

・判明した脆弱性と脆弱性がもたらす脅威

【CPSN-MCB271-*、CPSN-EOB471EI-□1、CPSN-PCB271-S1-041 共通】

① CVE-2026-82781:「CONPROSYS Nano シリーズにおけるクロスサイトスクリプティング」…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-2026-82782：「CONPROSYS Nano シリーズにおける境界外書込み」…CWE-787
Web ブラウザから不正な URL を指定することで境界外への書込みが行われる可能性があり、悪意のある攻撃者に利用されることで Web 設定機能が停止す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:N / A:L　　基本値：4.3

③ 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

④ CVE-2026-82783：「CONPROSYS Nano シリーズにおけるパスワードの平文保存」…CWE-256
パスワードが暗号化されずに保存されているため、悪意のある攻撃者に利用されることで情報が盗用される可能性があります。
CVSS:3.1 / AV:P / AC:H / PR:N / UI:N / S:U / C:L / I:N / A:N　　基本値：4.2

【CPSN-MCB271-*のみ】

① CVE-2026-82784:「CONPROSYS Nano シリーズにおける重要な機能に対する認証の欠如」…CWE-306
REST API に認証が適切に設定されておらず、悪意のある攻撃者に利用されることで情報が盗用される可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:N / UI:N / S:U / C:L / I:L / A:N　　基本値：6.5

② CVE-2026-82785：「CONPROSYS Nano シリーズにおけるスタックバッファオーバーフロー」…CWE-121
MQTT、SNMP の設定で入力内容の検証が不十分になっており、悪意のある攻撃者が不正なパラメータを送信することでシステムが停止す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:N / A:L　　基本値：4.3

③ CVE-2026-82786：「CONPROSYS Nano シリーズにおける資格情報の不十分な保護」
…CWE-522
バックアップファイルに機密情報（MQTT、REST API の認証情報）が含まれており、悪意のある攻撃者に利用されることで情報が盗用される可能性があります。
CVSS:3.1 / AV:N / AC:H / PR:L / UI:N / S:C / C:H / I:N / A:N　　基本値：6.3

・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。

- リモート I/O カプラユニット（サーバタイプ）（対策済みバージョン：Ver. 1.82 以降）
  https://www.contec.com/jp/products-services/daq-control/iiot-conprosys/remote-io/cpsn-mcb271-1-081/support/#firmware

- リモート I/O カプラユニット（EtherNet/IP アダプタ）（対策済みバージョン：Ver. 1.02 以降）
  https://www.contec.com/jp/products-services/daq-control/iiot-conprosys/remote-io/cpsn-eob471ei-41/support/#firmware

- プログラマブルリモート I/O カプラユニット（ソフト PLC タイプ）（対策済みバージョン：Ver. 1.61 以降）
  https://www.contec.com/jp/products-services/daq-control/iiot-conprosys/remote-io/cpsn-pcb271-s1-041/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⑤**

シリーズ名　：　CONPROSYS IO-Linkマスタ
製品名　　：　CONPROSYS IO-Linkマスタ
製品型式　　：　CPSL-08P1EN
バージョン　：　2.3.10 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-2026-82787：「IO-Link マスタにおける重要な機能に対する認証の欠落」…CWE-306
設定画面に認証が適切に設定されておらず、悪意ある攻撃者に利用されることで~~情報の盗用や改竄~~、悪意あるプログラムの実行が行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:H　　基本値：9.8

② CVE-2026-82788：「IO-Link マス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:N / AC:L / PR:N / UI:R / S:C / C:L / I:L / A:N　　基本値：6.1

③ CVE-2020-7746：「コンテック製品における脆弱な JavaScript ライブラリの使用」…CWE-1395
脆弱性を含む JavaScript ライブラリを使用しており、悪意ある攻撃者に利用されることで情報の盗用、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:N / S:U / C:N / I:N / A:H　　基本値：7.5

・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。

- CPSL-08P1EN（対策済みバージョン：Ver. 2.3.1.0 以降）
  https://www.contec.com/jp/download/contract/contract2/?itemid=b33a8f26-d915-4b65-8912-a45b607b4ee1&downloaditemid=dcea2d68-bfe3-4572-97d9-d045531c7f7f

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⑥

シリーズ名　：　CONPROSYS HMI SYSTEM
製品名　　：　CONPROSYS HMI System(CHS)
製品型式　　：　なし
バージョン　：　3.8.0 未満

<バージョンの確認方法>
ソフトウェアの画面右上から「ヘルプ」→「バージョン」を開くことで確認できます。

・判明した脆弱性と脆弱性がもたらす脅威

① CVE-2026-82789 :「CONPROSYS HMI SYSTEM(CHS)における Eval インジェクション」… CWE-95
演算式入力にて実行可能な任意の PHP コードを送信でき、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

・対策方法

コンテックの Web サイトにある最新のインストーラを反映することで上記脆弱性の対策を施したバージョン(Ver.3.8.0 以降)を利用可能です。
当社 Web サイトからのダウンロード申し込みページ：
(コンテックの Web サイトに CHS を検索するとページが表示されます。)
https://www.contec.com/jp/form/product1/?ItemOverview%20ItemCode=%E3%82%A4%E3%83%B3%E3%82%B9%E3%83%88%E3%83%BC%E3%83%A9%E7%94%B3%E8%BE%BC%E3%81%BF&ItemOverview%20ItemName=CONPROSYS+HMI+System

・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#96551518
https://jvn.jp/vu/JVNVU96551518/

■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