公開日　2026 年 11 月 06 日

株式会社コンテック

CONPROSYS 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 CONPROSYS 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。
対象製品を使用している場合は、対策済みバージョンへ更新してください。

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 ソフトウェア開発キット	CONPROSYS 拡張 SDK、CONPROSYS Linux SDK

対象製品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	4.2.0 未満
		M2M Gateway スタックタイプ	4.2.0 未満
		M2M コントローラコンパクトタイプ	4.2.0 未満
		M2M コントローラスタックタイプ	4.2.0 未満

・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。

- M2M Gateway コンパクトタイプ（対策済みバージョン：Ver. 4.2.0 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. 4.2.0 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. 4.2.0 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. 4.2.0 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

対象製品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	3.1.0 未満
		スタックタイプ	3.1.0 未満

・判明した脆弱性と脆弱性がもたらす脅威

① CVE-2026-109618：「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。

- コンパクトタイプ（対策済みバージョン：Ver. 3.1.0 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. 3.1.0 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　：　2.20 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-2026-109618：「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。

- CPS-TM341MB/GMB/G5MB（対策済みバージョン：Ver. 2.20 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

該当製品④

シリーズ名　：　CONPROSYS SDK
製品名　　：　CONPROSYS ソフトウェア開発キット
製品型式　　：　CONPROSYS Linux SDK
バージョン　：　1.5.1 未満、2.2.1 未満

・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

使用する SDK 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 SDK は当社 Web サイトから入手できます。
開発支援ツール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。

- CONPROSYS Linux SDK セルフビルド版（対策済みバージョン：2.2.1 以降）
https://www.contec.com/jp/download/contract/contract2/?itemid=59bbfcd1-3065-4901-8e38-f5f682d40515&downloaditemid=ed126593-45d3-4520-bc07-c422ff46ae96
- CONPROSYS Linux SDK セルフビルド版（対策済みバージョン：1.5.1 以降）
https://www.contec.com/jp/download/contract/contract2/?itemid=59bbfcd1-3065-4901-8e38-f5f682d40515&downloaditemid=8c4c95bd-a765-497f-bfb4-764c0e0b5909
- CONPROSYS Linux SDK クロスビルド版（対策済みバージョン：2.2.1 以降）
https://www.contec.com/jp/download/contract/contract2/?itemid=59bbfcd1-3065-4901-8e38-f5f682d40515&downloaditemid=c2572654-e93a-412d-ab02-3be8917a3118
- CONPROSYS Linux SDK クロスビルド版（対策済みバージョン：1.5.1 以降）
https://www.contec.com/jp/download/contract/contract2/?itemid=59bbfcd1-3065-4901-8e38-f5f682d40515&downloaditemid=735a7fa1-86bf-4988-bb32-6965928075ec

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、開発支援ツール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