

CONPROSYS HMI System(CHS)の脆弱性について

■概要

当社製の Web HMI/SCADA ソフトウェア「CONPROSYS HMI System(以下 CHS)」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・回避策を以下に示しますので、対策または軽減策・回避策の実施をお願いいたします。

■該当製品

製品名 : CONPROSYS HMI System(CHS)

バージョン : 3.7.7 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

【JVN#92266386】

- ① CVE-2025-34021 : 「CONPROSYS HMI System(CHS)におけるクロスサイトスクリプティングの脆弱性」…CWE-79
特定 PHP スクリプトのパラメータに記載した JavaScript コードを実行される脆弱性が存在しており、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:R/S:C/C:L/I:L/A:N 基本値 : 6.1
- ② CVE-2025-34040 : 「CONPROSYS HMI System(CHS)における情報漏えいの脆弱性」…CWE-215
本来公開不要なデバッグ情報が公開されている脆弱性があり、悪意ある攻撃者に機密情報が利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:N/A:N 基本値 : 5.3

■ 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.3.7.7 以降)を利用可能です。

コンテック サイトからのダウンロードページ：

(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/download/contract/contract4/?itemid=ea8039aa-3434-4999-9ab6-897aa690210c&downloaditemid=866d7d3c-aae9-438d-87f3-17aa040df90b>

■ 回避策

対策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

- ・ JNVNU#92266386「コンテック製 CONPROSYS HMI System(CHS)における複数の脆弱性」

<https://jvn.jp/vu/JNVNU92266386/>

■ 謝辞

本脆弱性の発見者である Converge Technology Solutions の Alex Williams 氏に厚く御礼申し上げます。

■ 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

- ・ 2025 年 07 月 01 日 初版