公開日　2023 年 1 月 20 日
改訂日　2023 年 1 月 24 日

株式会社コンテック

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と対策方法、回避策を以下に示します。対策または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：Ver.3.5.0 以下

■判明した脆弱性と脆弱性がもたらす脅威

【JVNVU#97195023】

CVE-2023-22324:「CONPROSYS HMI System(CHS)における複数の SQL インジェクションの脆弱性」

複数の設定画面に対し、特定のパラーメータを POST することで SQL コマンドを変更でき、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

■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.3.5.1 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、当社は以下に示す回避策を講じることを推奨します。

・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#97195023「コンテック製CONPROSYS HMI System (CHS)における複数のSQLインジェクションの脆弱性」

■謝辞

本脆弱性の発見者である Elex CyberSecurity, Inc. の Mosin 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/