公開日　2022 年 10 月 14 日
改訂日　2023 年 01 月 10 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)」において複数の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：① Ver.3.4.5 未満
　　②～⑤ Ver.3.5.0 未満

■判明した脆弱性と脆弱性がもたらす脅威

【JVNVU#96873821】

① CVE-2022-44456:「CONPROSYS HMI System(CHS)における OS コマンドインジェクションの脆弱性」
ネットワーク導通確認画面から OS が実行できるコマンドを入力することができ、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、悪意あるプログラムの実行等が行われる可能性があります。

② CVE-2023-22331:「CONPROSYS HMI System(CHS)における認証不備の脆弱性」
インストール直後は共通のアカウント(ユーザー名、パスワード)で動作する仕様になっており、このアカウントの設定をそのままにしておくと悪意ある攻撃者に利用されることで認証情報を変更される可能性があります。

③ CVE-2023-22334:「CONPROSYS HMI System(CHS)における情報漏洩の脆弱性」
CONPROSYS HMI System(CHS)の認証情報はハッシュ化されているものの
暗号化はされておらず悪意のある攻撃者に盗用される可能性があります。

④ CVE-2023-22373:「CONPROSYS HMI System(CHS)における JavaScript コード無効化処理が不十分な問題」
CONPROSYS HMI System(CHS)の JavaScript コード無効化処理に問題があり、悪意のあるページ編集者に利用されることで Web ブラウザに保存されている Cookie や認証情報を
盗用される可能性があります。

⑤ CVE-2023-22339:「CONPROSYS HMI System(CHS)におけるアクセス制限不備の脆弱性」
HTTPS 認証に利用できるサイト証明書が Web からアクセス可能となっており
悪意ある攻撃者が利用することで別の HTTPS で運用している CONPROSYS HMI

System(CHS)の通信を盗聴できる可能性があります。

■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.3.5.0 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。

【①～⑤に共通する回避策】

・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

【脆弱性個々における追加回避策】

②インストール後、admin/demo の各プロジェクトにログインし、初期パスワードを変更する

③HTTP での接続は控え、HTTPS で接続するように運用を変更する

⑤同梱のサイト証明書の利用を止め、新しく作成したサイト証明書に変更する

サイト証明書の更新にあたっては Web からアクセス不可な場所に設置する

■関連情報

・JVNVU#96873821「コンテック製CONPROSYS HMI System (CHS)における複数の脆弱性」

・ICS Advisory (ICSA-22-347-03)　Contec CONPROSYS HMI System (CHS)

■謝辞

本脆弱性の発見者である Radboud 大学の Floris Hendriks 氏、Jeroen Wijenbergh 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

2023 年 01 月 10 日　10 月 14 日に公開した脆弱性を①とし、②～⑤の内容を追記