公開日　2023 年 05 月 31 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、以下の影響を受ける恐れがあります。

・データの盗用や改竄

・悪意あるプログラムを実行しシステムを破壊される

・機能を停止させる

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。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

バージョン　：　3.5.3 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-2023-28713：「CONPROSYS HMI System(CHS)におけるパスワードの平文保存」…CWE-256

データベースのアカウントがローカルフォルダのファイルに平文で保存されており、悪意ある攻撃者に利用されることで情報の盗用・改竄が行われる可能性があります。

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N　　基本値：5.5

② CVE-2023-28399：「CONPROSYS HMI System(CHS)における重要なリソースに対する不適切なパーミッションの割り当て」…CWE-732

ソフトウェアがインストールされているローカルフォルダが明示的に ACL(Access Control List)を設定していないため、OS の一般ユーザーにも広範囲な権限を許可されています。

悪意ある攻撃者が一般ユーザーとしてログインすることで、システムの破壊、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:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H　　基本値：7.8

③ CVE-2023-28657：「CONPROSYS HMI System(CHS)における不適切なアクセス制御」…CWE-284
権限の低いユーザーが自分の権限を引き上げ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・改竄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:H/I:H/A:H　基本値：8.8

④ CVE-2023-28651：「CONPROSYS HMI System(CHS)における複数の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特定の JavaScript コードを保存させ、別の PHP をコールする時に前述の JavaScript 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・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:H/UI:R/S:C/C:L/I:L/A:N　基本値：4.8

⑤ CVE-2023-28824：「CONPROSYS HMI System(CHS)におけるサーバサイドのリクエストフォージェリの脆弱性」…CWE-918
クエリ設定画面で本来アクセスできない DB の内容にアクセスできる脆弱性があり、悪意ある攻撃者に利用されることで情報の盗用・改竄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

⑥ CVE-2023-29154：「CONPROSYS HMI System(CHS)における SQL インジェクション」…CWE-89
クエリ設定画面で特定のパラメータを POST することで SQL コマンドを実行できる脆弱性があり、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:H/UI:N/S:U/C:H/I:H/A:L　基本値：6.7

⑦ CVE-2023-2758：「CONPROSYS HMI System(CHS)におけるインタラクション頻度の不適切な制限」…CWE-799
不正な認証の繰り返しを制限するための処理が適切でなく、悪意ある攻撃者が HTTP ヘッダ内に特定の要素を含んだリクエストを繰り返すことで本システムへログインできない状況を作り出す可能性があります。
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L　基本値：3.7

■対策方法

ソフトウェアを最新版(Ver.3.5.3 以降)に更新してください。
最新のソフトウェアは当社 Web サイトより入手できます。
(当社 Web サイトで 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#93372935「コンテック製 CONPROSYS HMI SYSTEM(CHS)における複数の脆弱性」
https://jvn.jp/vu/JVNVU93372935/

■謝辞

本脆弱性の発見者である Michael Heinzl 氏（①～⑥）、Tenable, Inc.の Jimi Sebree 氏（⑦）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/tsc/

■改訂履歴

・2023 年 05 月 31 日　　初版