

CONPROSYS HMI System (CHS)の脆弱性について

■概要

当社の WEB HMI/SCADA ソフトウェア CONPROSYS HMI System (CHS)において、サーバ側の PHP コードに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可能性があります。この脆弱性の概要ならびに対策方法を説明します。

■判明した脆弱性と脆弱性がもたらす脅威

上記の製品の特定 PHP コードに、OS コマンドインジェクションというセキュリティ問題が存在することが判明しました。悪意を持つものがサーバの PHP にリクエストを送信する時に、OS コマンドを仕込まれることで、任意のコマンドを実行することができてしまう。本脆弱性は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可能性があります。インターネット上に公開している利用者につきましては緊急で対策が必要となります。

■対策方法

コンテックのホームページ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>

■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/>