Release date: Oct 14th, 2022

CONTEC CO., Ltd

Vulnerability Correction in CONPROSYS HMI System (CHS)

■ Overview

We have discovered a vulnerability in the server-side PHP code of our WEB HMI/SCADA software CONPROSYS HMI System (CHS). If this vulnerability is exploited by a malicious attacker, data may be stolen or tampered with, or a malicious program may be executed to destroy the system. The following is an overview of this vulnerability and countermeasures.

■ The vulnerability and its threat

It has been discovered that a security problem called OS Command Injection exists in the specific PHP code of the above products.

When a malicious entity sends a request to PHP on the server, an OS command can be embedded to execute arbitrary commands. If this vulnerability is exploited by an attacker, there is a possibility of data theft or falsification, execution of malicious programs, and system corruption.

For users who construct CHS server on the Internet, urgent countermeasures are required.

■ Fix Version

By installing the latest version on CONTEC's website, the above vulnerabilities can be fixed.

Download page from CONTEC site:

(You can find the page by search “CHS” on CONTEC website)

https://www.contec.com/download/contract/contract4/?itemid=ea8039aa-3434-4999-9ab6-897aa690210c&downloaditemid=866d7d3c-aae9-438d-87f3-17aa040df90b

After the version is install, the version number is Version3.4.5 (2022-10-13).

■ Contact Information

Technical Support Center

https://www.contec.com/support/technical-support/