Release date: July 1st, 2025

CONTEC CO., Ltd

# Vulnerability Correction in CONPROSYS HMI System (CHS)

## ■ Overview

Contec has identified several vulnerabilities in its CONPROSYS HMI System (CHS) Web HMI/SCADA software.

**These vulnerabilities could be exploited by a malicious attacker to steal.**

**- Stealing or tampering with data**

**- Execution of malicious programs that could result in destruction of the system**

**- Deactivation of certain functions**

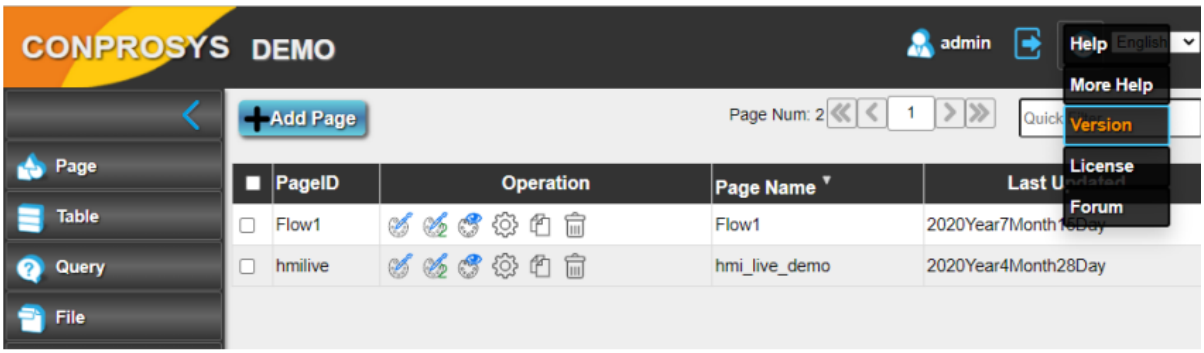
The products affected by these vulnerabilities and the countermeasures/workarounds are listed below. Please implement the appropriate countermeasures or workarounds as soon as possible.

## ■ Affected products

Model: CONPROSYS HMI System(CHS)

Version: Less than Ver.3.7.7

< Checking the version> To check the version, navigate to ¥[Help] > ¥[Version] in the upper-right corner of the software screen.




## ■ The vulnerability and its threat

【JVNVU#92266386】

1. CVE-2025-34080: "Cross-site Scripting Vulnerability in CONPROSYS HMI System (CHS)"... CWE-79

   This vulnerability allows JavaScript code specified in the parameters of certain PHP scripts to be executed. This vulnerability can be exploited by malicious attackers to steal or tamper with information, or execute malicious programs.

   CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N  Basic Score: 6.1

2. CVE-2025-34081: "Information Disclosure Vulnerability in CONPROSYS HMI System (CHS)"...
   CWE-215
   This vulnerability allows debugging information that should not be disclosed to be exposed, potentially allowing a malicious attacker to use confidential information.
   CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Basic Score: 5.3

## ■ Fix Version

Update the software to the latest version (Ver. 3.7.7 or later). The latest software is available from the Contec website.
(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

## ■ Workarounds

For customers unable to update to the latest version, Contec recommends the following workarounds to minimize the risk of exploitation of these vulnerabilities by an attacker.
- Disconnect the product from the network.
- Set up a firewall at an upstream location in the network where the product is being used.
- Limit network access for this product to a reliable closed network.

## ■ Related Information

- JVNVU#92266386 "Multiple vulnerabilities in Contec's CONPROSYS HMI System (CHS)"
https://jvn.jp/vu/JVNVU92266386/

## ■ Acknowledgments

Contec would like to thank Alex Williams of Converge Technology Solutions.

## ■ Contact Information

Technical Support Center
https://www.contec.com/jp/support/technical-support/

## ■ Revision History

July 1st, 2025 The first edition
July 2nd, 2025 Correct the CVE number