Release date: May 31th, 2023

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.

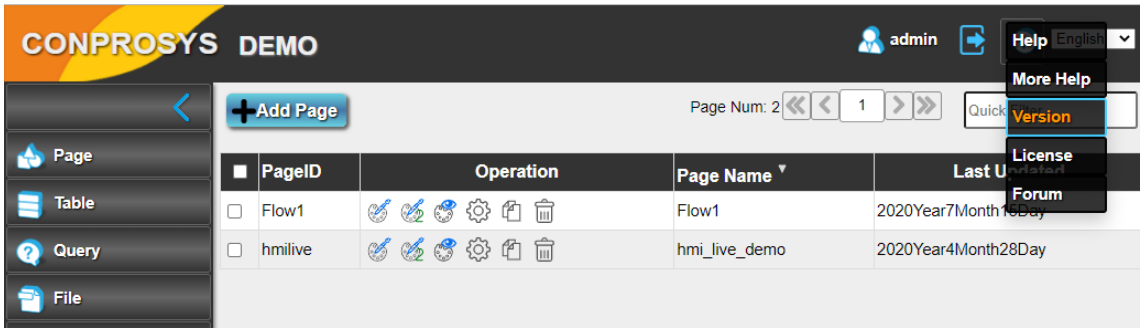
■ Affected products

Model: CONPROSYS HMI System (CHS)

Version: Less than Ver.3.5.3

< 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

1. CVE-2023-28713: ”Plain text storage of passwords in CONPROSYS HMI System (CHS)”…CWE-256
   Database account details are stored in a plain text file in a local folder, allowing malicious attackers to steal or tamper with information.
   CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N Basic Score: 5.5

2. CVE-2023-28399: ”Incorrect permission assignment for critical resource in CONPROSYS HMI System (CHS)”…CWE-732
   Because there is no specific Access Control List (ACL) set for the local folder where the software is installed, even general OS users are permitted a wide range of permissions. This makes it possible for malicious attackers to destroy the system or execute malicious programs when logged in as general users.
   CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Basic Score: 7.8

3. CVE-2023-28657: ”Improper access control in CONPROSYS HMI System (CHS)”…CWE-284
   This vulnerability allows users with low-level privileges to raise their privilege level, allowing malicious attackers to steal or tamper with information.
   CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Basic Score: 8.8

4. CVE-2023-28651: ”Multiple cross-site scripting vulnerabilities in CONPROSYS HMI System (CHS)”…CWE-79
   This vulnerability allows specific JavaScript code to be stored in the parameters of a specific PHP script so that the JavaScript code is executed when a separate PHP call is performed, allowing malicious attackers to steal or tamper with information or execute malicious programs.
   CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N Basic Score: 4.8

5. CVE-2023-28824: ”Server-side request forgery vulnerability in CONPROSYS HMI System (CHS)”…CWE-918
   This vulnerability makes it possible to access DB content that is not originally accessible from the query settings screen, allowing malicious attackers to steal or tamper with information.
   CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N Basic Score: 4.3

6. CVE-2023-29154: ”SQL injection in CONPROSYS HMI System (CHS)”…CWE-89
   This vulnerability makes it possible to execute SQL commands by changing specific parameters using POST in the query settings screen, allowing malicious attackers to steal information.
   CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L Basic Score: 6.7

7. CVE-2023-2758: ”Improper control of interaction frequency in CONPROSYS HMI System (CHS)”…CWE-799
   Due to improper processes for restricting repeated invalid authentication actions, this vulnerability could allow malicious attackers to make it impossible to log into the system by repeatedly making requests with specific elements in the HTTP header.
   CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L Basic Score: 3.7

■ Fix Version

Update the software to the latest version (Ver. 3.5.3 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#93372935 “Multiple vulnerabilities in Contec CONPROSYS HMI System (CHS)”
https://jvn.jp/en/vu/JVNVU93372935/

■ Acknowledgments

Contec would like to thank Michael Heinzl for identifying vulnerabilities 1 through 6, and Jimi Sebree of Tenable, Inc. for identifying vulnerability 7.

■ Contact Information

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

■ Revision History

May 31th, 2023 The First Edition