Release date: Oct 14th, 2022

Revision date: Jan 10th, 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 or tamper with data or to execute malicious programs that could result in the destruction of the system.

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： (1) Less than Ver.3.4.5

(2) to (5) Less than Ver.3.5.0

■ The vulnerability and its threat

[JVNVU#96873821]

(1) CVE-2022-44456: “CONPROSYS HMI System (CHS) OS command injection vulnerability”

This vulnerability makes it possible for OS execution commands to be input from the network continuity confirmation screen. These commands could then be used by a malicious attacker to steal or tamper with information, destroy the system, or execute malicious programs.

(2) CVE-2023-22331: “CONPROSYS HMI System (CHS) authentication failure vulnerability”

CONPROSYS HMI System (CHS) is designed to use a common account (user name/password) immediately after installation. If this account setting is left unchanged, this vulnerability could be used by a malicious attacker to alter the authentication information.

(3) CVE-2023-22334: “CONPROSYS HMI System (CHS) information leakage vulnerability”
Because the authentication information for CONPROSYS HMI System (CHS) is hashed but unencrypted, this vulnerability could be used by a malicious attacker to steal authentication information.

(4) CVE-2023-22373: “Incomplete CONPROSYS HMI System (CHS) JavaScript code deactivation process”
Due to an incomplete JavaScript code deactivation process in CONPROSYS HMI System (CHS), a malicious attacker could use page editing tools to steal cookies and authentication information stored in the Web browser being used.

(5) CVE-2023-22339: “CONPROSYS HMI System (CHS) improper access control vulnerability”
Site certificates used for HTTPS authentication are accessible from the Web. This vulnerability could be used by a malicious attacker to eavesdrop on CONPROSYS HMI System (CHS) communications operating on a different HTTPS.

■ Fix Version

By installing the latest version (less than ver.3.5.0) 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/jp/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.

[Workarounds for vulnerabilities (1) through (5)]

- 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.

[Additional workarounds for specific vulnerabilities]

(2) After installation, log in to each project using the admin/demo account and change the default password.

(3) Change the settings so that connections use HTTPS instead of HTTP.

(5) Stop using the included site certificate and create a new site certificate for use. When renewing the site certificate, save it in a location that cannot be accessed from the Web.

■ Related information

・JVNVU#96873821 "Contec CONPROSYS HMI System (CHS) multiple vulnerabilities"
・ICS Advisory (ICSA-22-347-03)　Contec CONPROSYS HMI System (CHS)

■ Acknowledgments

Contec would like to thank Floris Hendriks and Jeroen Wijenbergh of Radboud University for identifying these vulnerabilities.

■ Contact Information

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

■ Revision history

January 10, 2023: Specified the vulnerability disclosed on October 14 as vulnerability (1) and added information for vulnerabilities (2) through (5).