Release date: Mar 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.

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: Ver.3.5.1 and earlier

■ The vulnerability and its threat

[JVNVU#92145493]

CVE-2023-1658: ”CONPROSYS HMI System (CHS) SQL injection vulnerability”

Changing specific parameters using POST makes it possible to change SQL commands for HTTP header, allowing malicious attackers to steal information.

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Basic Score: 7.5

■ Fix Version

By installing the latest version (Ver.3.5.2 or later) 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

■ 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.

- 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#92145493 “CONPROSYS HMI System (CHS) SQL injection vulnerability”
  https://jvn.jp/en/vu/JVNVU92145493/

■ Acknowledgments

Tenable Network Security, reported the vulnerability to Contec Co., Ltd.

■ Contact Information

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