Yokogawa Security Advisory Report

YSAR-24-0002

Published on June 17, 2024
Last updated on July 4, 2024

YSAR-24-0002: DLL Hijacking Vulnerability in CENTUM CAMS Log server

Overview:

DLL Hijacking vulnerability has been found in CENTUM CAMS Log server. Yokogawa has identified the range of affected products in this report.
Please review the report and confirm which products are affected to implement security measures for the overall systems. Please consider applying the countermeasures as needed.

Affected Products:

This vulnerability affects the following products.
• CENTUM series

CENTUM CS 3000	R3.08.10 - R3.09.50	LHS1100/LHM1101 Standard Operation and Monitoring Function (Affected even if CAMS is not enabled)
CENTUM VP	R4.01.00 - R4.03.00 R5.01.00 - R5.04.20	LHS1100/LHM1101 Standard Operation and Monitoring Function (Affected even if CAMS is not enabled)
	R6.01.00 - R6.11.10	VP6H1100 Standard Operation and Monitoring Function (Affected even if CAMS is not enabled)

Vulnerability:

If an attacker is somehow able to intrude into a computer that installed affected product or access to a shared folder, by replacing the DLL file with a tampered one, it is possible to execute arbitrary programs with the authority of the SYSTEM account.

CWE-284 : Improper Access Control
CVE: CVE-2024-5650
CVSS v3 Base score: 8.5
CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Countermeasures:

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM CS 3000	R3.08.10 - R3.09.50	None	No patch software will be available because these products are already end of support. Please consider system upgrade to the latest revision of CENTUM VP.
CENTUM VP	R4.01.00 – R4.03.00	None	
	R5.01.00 - R5.04.20	None	
	R6.01.00 – R6.11.10	R6.11.12	Please revision up to the R6.11.10 and apply patch software (R6.11.12).

Yokogawa recommends updating as above the countermeasures. When Yokogawa service personnel perform update, those charges are borne by the customer.

Yokogawa strongly recommends all customers to establish and maintain a full security program, not only for the vulnerability identified in this YSAR. Security program components are: Patch updates, Anti-virus, Backup and recovery, zoning, hardening, whitelisting, firewall, etc. Yokogawa can assist in setting up and running the security program continuously. For considering the most effective risk mitigation plan, as a starting point, Yokogawa can perform a security risk assessment.

Supports:

For questions related to this report, please contact the below.
https://contact.yokogawa.com/cs/gw?c-id=000498

Reference:

1. Common Vulnerability Scoring System (CVSS)
   https://www.first.org/cvss/
   CVSS is a common language for scoring IT vulnerabilities independent from any vendors. It provides an open framework for communicating the characteristics and impacts of IT vulnerabilities, scaling it in numeric scores.
   The CVSS scores described in this report are provided “AS IS.” Yokogawa has no guarantee over the scores, and the severity caused by the vulnerabilities has to be judged by the users considering the security measures equipped with the overall systems.

Revision History:

June 17, 2024: 1st Edition
July 4, 2024: 2rd Edition Added note of caution

* Contents of this report are subject to change without notice.