

# Yokogawa Security Advisory Report

YSAR-22-0006

Published on May 27, 2022

Last updated on July 27, 2022

---

## YSAR-22-0006: Data breach / falsification and resource exhaustion vulnerability in CAMS for HIS

---

### Overview:

A vulnerability has been found in CAMS for HIS. Yokogawa has identified the range of affected products in this report.

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 (Including CENTUM CS 3000 Entry Class)	R3.08.10 - R3.09.00	These vulnerabilities affect this product if LHS4800(CAMS for HIS) is installed.
CENTUM VP (Including CENTUM VP Entry Class)	R4.01.00 - R4.03.00	These vulnerabilities affect this product if CAMS function is used.
	R5.01.00 - R5.04.20	These vulnerabilities affect this product regardless of whether CAMS function is used or not
	R6.01.00 - R6.09.00	

- Exaopc (R3.72.00 - R3.80.00) (These vulnerabilities affect this product if NTPF100-S6 "For CENTUM VP Support CAMS for HIS" is installed.)

- B/M9000CS (R5.04.01 - R5.05.01)

- B/M9000 VP (R6.01.01 - R8.03.01)

- 

### Vulnerability:

If an attacker is somehow able to intrude into a computer that installed the product, data managed by another CAMS for HIS may be breached / falsified using the account and password stored in that computer. And resource exhaustion attack could be launched to create unnecessary files on another CAMS for HIS, finally disabling CAMS for HIS functions using the account and password stored in that computer.

Violation of Secure Design Principles ([CWE-657](#))

CVE: [CVE-2022-30707](#)

CVSS v3 Base score: 6.4

[CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H](#)

**Countermeasures:**

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM CS 3000 CENTUM CS 3000 Entry Class	R3.08.10 - R3.09.00	-	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 CENTUM VP Entry Class	R4.01.00 - R4.03.00		
	R5.01.00 - R5.04.20		
	R6.01.00 - R6.09.00	R6.09.03	Please revision up to the R6.09.00 and applying patch software (R6.09.03).
Exaopc	R3.72.00 - R3.80.00	R3.80.01	Please revision up to the R3.80.00 and applying patch software (R3.80.01).
B/M9000CS	R5.04.01 - R5.05.01	-	This product is not affected by the vulnerabilities. However, this product is affected by the existence of CENTUM installed on the same PC. If installed CENTUM need to update, also please update B/M9000 to suitable revision.
B/M9000 VP	R6.01.01 - R8.03.01		

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>

**Acknowledgement:**

The vulnerabilities were discovered and notified by the following organizations and persons.

- Jacob Baines from Dragos, Inc

**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 have to be judged by the users considering the security measures equipped with the overall systems.

**Revision History:**

May 27, 2022: 1<sup>st</sup> Edition

July 27, 2022: 2nd Edition: Added CVE

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