

Yokogawa Security Advisory Report

YSAR-20-0001

Published on July 31, 2020

Last updated on December 2, 2020

YSAR-20-0001: Vulnerabilities in CAMS for HIS

Overview:

Vulnerabilities have been found in CAMS for HIS of CENTUM. 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:

These vulnerabilities affect the following products.

- CENTUM series

CENTUM CS 3000 (Including CENTUM CS 3000 Entry Class)	(R3.08.10 - R3.09.50)	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 - R6.07.00)	

- Exaopc (R3.72.00 - R3.78.00) (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:

The following vulnerabilities have been found in CAMS for HIS. These vulnerabilities may allow a remote unauthenticated attacker to create or overwrite any file, run any commands.

- Improper Authentication ([CWE-287](#))

[CVE-2020-5608](#)

CVSS v3 Base score: 8.1

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

This vulnerability may allow a remote unauthenticated attacker to send tampered communication packets.

- Path Traversal ([CWE-22](#))

[CVE-2020-5609](#)

CVSS v3 Base score: 8.1

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

This vulnerability may allow a remote attacker to create or overwrite any file, run any commands.

Countermeasures:

By updating to the latest revision or applying the patch, the vulnerabilities is corrected.

Products	Affected Revisions	Countermeasures
CENTUM CS 3000 (Including CENTUM CS 3000 Entry Class)	R3.08.10 - R3.09.50	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 (Including CENTUM VP Entry Class)	R4.01.00 - R4.03.00	Please consider revision up to the latest revision (R5.04.20) and applying patch software (R5.04.D1). Please consider revision up to the latest revision (R6.07.00) and applying patch software (R6.07.11).
	R5.01.00 - R5.04.20	
	R6.01.00 - R6.07.00	
Exaopc	R3.72.00 - R3.78.00	It has been remediated in R3.78.10. Please update to R3.78.10 or later.
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 CS 3000 installed on the same PC. If installed CENTUM CS 3000 need to update, also please update B/M9000CS to suitable revision.
B/M9000 VP	R6.01.01 - R8.03.01	This product is not affected by the vulnerabilities. However, this product is affected by the existence of CENTUM VP installed on the same PC. If installed CENTUM VP need to update, also please update B/M9000 VP to suitable revision.

When Yokogawa service personnel perform revision up or install patches, 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.

Patching is by far the best protection against this vulnerability being exploited, but if for example for operational reason, patching is not possible. Yokogawa specialist can consult on the best course of action.

Supports:

For questions related to this report, please contact the below.

<https://contact.yokogawa.com/cs/gw?c-id=000498>

ACKNOWLEDGMENTS:

Yokogawa sincerely thanks the following party.
Nataliya Tilyapova and Ivan Kurnakov, Positive Technologies

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:

July 31, 2020	1 st Edition
September 4, 2020	2 nd Edition: Update Affected Products information.
December 2, 2020	3 rd Edition: Add Exaopc as affected product. Correct Affected Products information.

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