

Yokogawa Security Advisory Report

YSAR-22-0001

Published on January 7, 2022

Last updated on February 9, 2022

YSAR-22-0001: Vulnerabilities in CENTUM and Exaopc

Overview:

Vulnerabilities have been found in CENTUM and Exaopc. 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 - R3.09.00 (*)	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 - R6.08.00	

*: These products are not affected by vulnerability 1 and 2 below.

- Exaopc (R3.72.00 - R3.79.00) (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)

Vulnerability1 (Hard Code Vulnerability in OS Account Credentials):

If the password for the OS account created when installing the product has not been changed from the default password, and the hard-coded credentials (default password) for the account are used to unauthorized login to the computer that installed the product, there is a possibility that files and shared memory in the system will be accessed.

The product is not affected by this vulnerability if the default password of that account has been properly changed after installation.

Use of Hard-coded Credentials ([CWE-798](#))

[CVE-2022-21194](#)

CVSS v3 Base score: 7.1

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

Vulnerability2 (Hard Code Vulnerability in CMAS server Credentials):

If the hard-coded credentials for CAMS server application are used to send a malformed packet to CAMS server, all functions of CAMS server can be abused, including suppressing alarms.

Use of Hard-coded Credentials ([CWE-798](#))

[CVE-2022-23402](#)

CVSS v3 Base score: 7.8

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

Vulnerability3 (Vulnerability in CMAS for HIS server):

If CAMS for HIS server receives a malformed packet, the following incidents may occur with user permissions running the service.

- Any file on CAMS for HIS server will be read.
- Arbitrary files are created/overwritten in any location on CAMS for HIS server.
- Arbitrary commands will be executed on CAMS for HIS server.

Relative Path Traversal ([CWE-23](#))

[CVE-2022-21808](#), [CVE-2022-22729](#)

Authentication Bypass by Assumed-Immutable Data ([CWE-302](#))

CVSS v3 Base score: 7.1

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

Vulnerability4 (Vulnerability in CMAS for HIS log server):

If CAMS for HIS log server receives a malformed packet, the following incidents may occur with user privileges running the service.

- CAMS for HIS log server crashes.
- Arbitrary log files are created/overwritten in any location in CAMS for HIS log server.
- Creating invalid logs on CAMS for HIS log server makes it difficult to analyze the logs when problems occur.

Improper Output Neutralization for Logs ([CWE-117](#))

Relative Path Traversal ([CWE-23](#))

Uncontrolled Resource Consumption ([CWE-400](#))

[CVE-2022-22151](#), [CVE-2022-21177](#), [CVE-2022-22145](#)

CVSS v3 Base score: 5.9

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

Vulnerability5 (Inappropriate access privilege vulnerability in Root Service function):

If an attacker is somehow able to intrude into a computer that installed the product, the named pipe created by Root Service function may have inappropriate access privileges, which may allow arbitrary programs to be executed with the system privileges running the process.

OS Command Injection ([CWE-78](#))

[CVE-2022-22148](#)

CVSS v3 Base score: 8.6

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

Vulnerability6 (Inappropriate access privilege vulnerability in Long-term Data Archive Package):

If an attacker is somehow able to intrude into a computer that installed the product, the named pipe created by Long-term Data Archive Package may have inappropriate access privileges, arbitrary files may be deleted with the system privileges running the process.

Permissions, Privileges, and Access Controls ([CWE-264](#))

[CVE-2022-22141](#)

CVSS v3 Base score: 6.6

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

Vulnerability7 (DLL planting vulnerability):

CENTUM and Exaopc have a DLL injection vulnerability using the vulnerability 1 and a DLL planting vulnerability using the DLL search order vulnerability. For more details, please refer to the following.

<https://msrc-blog.microsoft.com/2018/04/10/triaging-a-dll-planting-vulnerability-2/>

Uncontrolled Search Path Element ([CWE-427](#))

[CVE-2022-23401](#)

CVSS v3 Base score: 8.3

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

Countermeasures:

- Countermeasure for Vulnerability1 (Hard Code Vulnerability in OS Account Credentials)
Follow the installation instructions for each product and change the password of the OS account created when installing the product to an appropriate one.

The initial password is set by default for the predefined user accounts in CENTUM VP and Exaopc. Be sure to change the initial password.

When changing the password, ensure that the same password is set in the entire system.

For more information about lists of the predefined user accounts in CENTUM VP and how to change the password for a user account, refer to: "CENTUM VP Security Guide"

- Countermeasure for Vulnerability 2 - 7

	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 - R6.08.00	R6.09.00	Please update to R6.09.00 or later.
Exaopc	R3.72.00 - R3.79.00	R3.80.00	Please update to R3.80.00 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 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:

Yokogawa thanks to the following organizations and persons for their support and cooperation in finding these vulnerabilities.

- 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:

January 7, 2022:	1 st Edition
January 12, 2022:	Correction of errors in “Countermeasures”
February 9, 2022:	Add CVE

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