Yokogawa Security Advisory Report

YSAR-23-0001

Published on April 5, 2023
Last updated on April 5, 2023

YSAR-23-0001: Elevation of Privilege Vulnerability in CENTUM Authentication Mode

Overview:

Elevation of Privilege vulnerability has been found in CENTUM Authentication Mode which is one of User Authentication Modes 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:

This vulnerability affects the following products.

• CENTUM series

CENTUM CS 1000	R2.01.00 - R3.09.50	
CENTUM CS 3000 (Including CENTUM CS 3000 Entry Class)		
CENTUM VP (Including CENTUM VP Entry Class)	R4.01.00 - R4.03.00	This vulnerability affects this product if CENTUM Authentication Mode is used.
	R5.01.00 - R5.04.20	
	R6.01.00 or later	

• Exaopc

R1.01.00 - R1.20.00 R2.01.00 - R2.10.00	
R3.01.00 or later	This vulnerability affects this product if CENTUM Authentication Mode is used.

• B/M9000CS (R5.04.01 - R5.05.01)
• B/M9000 VP (R6.01.01 - R7.04.51, R8.01.01 or later)

Vulnerability:

• Prerequisite
- CENTUM Authentication Mode is used for user authentication. (CENTUM VP, Exaopc)
- An attacker has somehow obtained the credentials of the computer on which the product is installed.

If an attacker is somehow able to intrude into a computer that installed the product or access or gain access to a shared folder, by tampering with the password file stored on that computer, it is possible to elevate the privileges of the user managed by CENTUM.
As a result, the control system may be operated by a higher-level privilege.

CWE-312 : Cleartext Storage of Sensitive Information
CVE: CVE-2023-26593
CVSS v3 Base score: 6.5
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Countermeasures:

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM CS 1000 CENTUM CS 3000 CENTUM CS 3000 Entry Class	R2.01.00 - 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 CENTUM VP Entry Class	R4.01.00 – R4.02.00	R4.03.00	Please revision up to the R4. 03. 00 and change the user authentication mode to Windows Authentication Mode. (*)
	R4.03.00	-	Change the user authentication mode to Windows Authentication Mode. (*)
	R5.01.00 - R5.04.20	-	
	R6.01.00 or later	-	
Exaopc	R1.01.00 - R1.20.00 R2.01.00 - R2.10.00	-	Please revision up to the R3. 07. 00 or later and change the user authentication mode to Windows Authentication Mode. (*)
	R3.01.00 or later	R3.70.00	
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		

*Changing to Windows Authentication Mode requires engineering work.
If the customer wishes to change to Windows Authentication Mode, please ask our sales or service staff.
Change 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.

- Denis Alimov (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:
April 5, 2023: 1st Edition

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