Yokogawa Security Advisory Report

YSAR-26-0003

Published on March 27, 2026
Last updated on March 27, 2026

YSAR-26-0003: Hardcoded Password Vulnerability in CENTUM

Overview:

Hardcoded Password Vulnerability have been found in CENTUM. 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 your overall systems. Please consider applying the countermeasures as needed.

Affected Products:

This vulnerability affects the following products.
• CENTUM series

	Affected Revisions	Affected Function
CENTUM VP	R5.01.00 - R5.04.20	LHS1100/LHM1101 Standard Operation and Monitoring Function (Affected when CENTUM Authentication Mode is used)
	R6.01.00 - R6.12.00	VP6H1100 Standard Operation and Monitoring Function (Affected when CENTUM Authentication Mode is used)
	R7.01.00	VP7H1100 Standard Operation and Monitoring Function (Affected when CENTUM Authentication Mode is used)

Vulnerability:

Affected products contain a hardcoded password for the user account (PROG) used for CENTUM Authentication Mode within the system. Under the following conditions, there is a risk that an attacker could log in as the PROG user.
The default permission for the PROG users is S1 permission (equivalent to OFFUSER). Therefore, for properly permission-controlled targets of operation and monitoring, even if an attacker user in as the PROG user, the risk of critical operations or configuration changes being performed is considered low. (If the PROG user's permissions have been changed for any reason, there is a risk that operations or configuration changes may be performed under the modified permissions. The CVSS values below are for the default permissions.)
Additionally, exploiting this vulnerability requires an attacker to already have access to the HIS screen controls. Therefore, an attacker can already operate and monitor at that point, regardless of this vulnerability.

The conditions under which this vulnerability is exploited:
If all of the following conditions are met, the affected products are vulnerable to this vulnerability.
- An attacker obtains the hardcoded password using a certain method.
- The HIS with the affected product installed is configured in CENTUM Authentication mode.
- An attacker must have direct access to the aforementioned HIS or be able to break into it remotely using a certain method and perform screen operations.

CWE-259 : Use of Hard-coded Password
CVE: CVE-2025-7741

CVSS v3 Base score: 4.0
CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v4 Base score: 2.1
CVSS:4.0/AV:L/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Countermeasures:

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM VP	R5.01.00 - R5.04.20	-	Change the user authentication mode to Windows Authentication Mode. (*)
	R6.01.00 - R6.12.00		
	R7.01.00	R7.01.10	Please apply patch software (R7.01.10).

*Changing to Windows Authentication Mode requires engineering work.
If the customer wishes to change to make this change, please ask our sales or service staff.
The customer will be responsible for the change costs.

 # Regarding the vulnerabilities described in this report
The vulnerabilities described in this report do not constitute non-conformities of the affected products. Therefore, if a customer requests Yokogawa to perform work related to the countermeasures described in this report, the associated costs will be borne by the customer.

 # Recommendation for countermeasures
To help reduce cybersecurity risks, Yokogawa recommends applying the countermeasures described in this report.
However, the actual impact of the vulnerabilities described in this report may vary depending on each customer's system environment. We recommend that customers carefully review this report and determine whether and when to apply the countermeasures based on a risk assessment of their system environment.

Yokogawa offers support for applying the countermeasures described in this report, as well as assistance with other cybersecurity measures. Please contact your local Yokogawa supporting office for further information or assistance.

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 customer considering the security measures equipped with the overall systems.

Revision History:
March 27, 2026: 1st Edition

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