Yokogawa Security Advisory Report

YSAR-22-0004

Published on March 10, 2022
Last updated on April 26, 2022

YSAR-22-0004: Vulnerabilities in CENTUM and ProSafe-RS

Overview:

Vulnerabilities have been found in CENTUM and ProSafe-RS. 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:

- Products affected by the following Vulnerability1

CENTUM VP (Including CENTUM VP Entry Class)	R4.01.00 - R4.03.00	These vulnerabilities affect this product if VP6E5150(Graphic Builder) is installed.
B/M9000 VP	R6.01.01 - R6.03.02	

- Products affected by the following Vulnerability2

CENTUM VP (Including CENTUM VP Entry Class)	R6.01.10 - R6.09.00	These vulnerabilities affect this product if VP6E5000(AD Suite Engineering Server Function) is installed.
ProSafe-RS	R4.01.00 – R4.07.00	These vulnerabilities affect this product if RS4E5000 (AD Suite Engineering Server Function) is installed.
B/M9000 VP	R8.01.01 - R8.03.01	

- Products affected by the following Vulnerability3

CENTUM VP (Including CENTUM VP Entry Class)	R6.01.10 - R6.07.10	These vulnerabilities affect this product if VP6E5000, VP6E5100(AD Suite Engineering Server Function, Standard Engineering Function) is installed.
ProSafe-RS	R4.01.00 – R4.05.00	These vulnerabilities affect this product if RS4E5000, RS4E5100 (AD Suite Engineering Server Function, Safety System Engineering & Maintenance Function) is installed.
B/M9000 VP	R8.01.01 - R8.03.01	

Vulnerability1 (Vulnerability in Graphic Builder):

If an attacker is somehow able to intrude into a computer that installed the product, by tampering with the files generated by the graphic builder, which may allow arbitrary programs to be executed on a computer that installed Standard Operation and Monitoring Function (HIS).

OS Command Injection (CWE-78)
CVE-2022-27188
CVSS v3 Base score: 6.1
CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:H

Vulnerability2 (Vulnerability in AD Suite Communication Protocol):

Improper authentication of the communication protocol provided by AD (Automation Design) server allows an attacker to use the functions provided by AD server. This may lead to leakage or tampering of data managed by AD server.

Improper Authentication (CWE-287)
CVE-2022-26034
CVSS v3 Base score: 6.4
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L

Vulnerability3 (Vulnerability in AD Suite Version Management Function):

If AD Suite Version Management Function is subjected to a DoS attack with malformed packets, the functions provided by AD server may stop.

NULL Pointer Dereference (CWE-476)
CVE-2019-0203
CVSS v3 Base score: 7.5
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Improper Input Validation (CWE-20)
CVE-2018-11782
CVSS v3 Base score: 6.5
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Resource Management Errors (CWE-399)
CVE-2015-0248
CVSS v3 Base score: 5.3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Countermeasures:

- Countermeasure for Vulnerability 1

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM VP CENTUM VP Entry Class	R4.01.00 - R4.03.00	-	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. * Vulnerability has been fixed in R5.01.00.

- Countermeasure for Vulnerability 2

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM VP CENTUM VP Entry Class	R6.01.10 – R6.09.00	R6.09.04	Please revision up to the R6.09.00 and applying patch software (R6.09.04).
ProSafe-RS	R4.01.00 – R4.07.00	R4.07.02	Please revision up to the R4.07.00 and applying patch software (R4.07.02).

*In below environments, there are some precautions to be taken when applying patch software.
Please be sure to check patch software install manual for details before applying patch software.
- Environment where both CENTUM VP and ProSafe-RS are installed.
- Environment where CENTUM VP’s AD (Automation Design) server and PRM are linked
- Environment where ProSafe-RS’s AD (Automation Design) server and PRM are linked

- Countermeasure for Vulnerability 3

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM VP CENTUM VP Entry Class	R6.01.10 – R6.07.10	R6.08.00	Please update to R6.08.00 or later.
ProSafe-RS	R4.01.00 – R4.05.00	R4.06.00	Please update to R4.06.00 or later.

- Countermeasure of B/M9000 VP

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.

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.

- FSTEC of Russia

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:

March 10, 2022:	1st Edition
March 16, 2022:	Added precautions for countermeasures
April 26, 2022:	Added affected products

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