Yokogawa Security Advisory Report

YSAR-14-0001E
Published on March 7, 2014
Last updated on December 22, 2017

YSAR-14-0001E: Vulnerabilities in CENTUM and other Yokogawa products

Overview:

On March 7, 2014, Yokogawa announced that any computer on which a CENTUM CS 3000 Integrated Production Control System is installed has three buffer overflow vulnerabilities. Since then, an additional vulnerability (”Vulnerability 4 - Simulator Management Process in the Expanded Test Functions”) has been found. Now that Yokogawa has investigated the scope of products that could be influenced by the four vulnerabilities and the countermeasures are summarized in this document.

Go over the report and confirm which products are affected in order to consider security measures for the overall systems. Also please consider applying the countermeasures introduced here as needed.

Affected Products:

Following are the products that would be affected by the vulnerabilities reported in this document.
Any computer on which these products are installed has vulnerabilities.

The following products are affected by Vulnerabilities 1 to 4.
CENTUM CS 1000, CENTUM CS 3000, CENTUM CS 3000 Entry Class,
CENTUM VP, CENTUM VP Entry Class,
Exaopc, B/M9000CS, B/M9000 VP

The following products are affected only by Vulnerability 1.
ProSafe-RS, Exapilot, Exaplog, Exaquantum, Exaquantum/Batch, Exasmoc, Exarqe,
AAASuite, PRM, STARDOM FCN/FCJ OPC Server for Windows,
Field Wireless Device OPC Server, DAQOPC, DAQOPC for DARWIN,
FieldMate, EJXMVTool, RPO Production Supervisor VP,
CENTUM Event Viewer Package,
CENTUM Long-term Trend Historian,
OmegaLand/OPC server interface module

For details of their revisions, please see <Table 1: List of Products affected by Vulnerabilities and Countermeasures>.

Vulnerability 1 – Operation Logging Process:

On a computer where the affected product(s) is installed, if a certain communication frame is transmitted to operation logging process, a buffer overflow occurs and the logging function is disabled. There is a potential risk that successful exploitation of this vulnerability allows remote attackers to execute arbitrary code with system privilege.

CVSS Base Score: 9.3, Temporal Score: 7.7.
** As for Common Vulnerability Scoring System (CVSS), see the references below:*
Access Vector: Network
Access Complexity: Medium

Authentication:	None
Confidentiality Impact (C):	Complete
Integrity Impact (I):	Complete
Availability Impact (A):	Complete
Exploitability:	Functional
Remediation Level:	Official Fix
Report Confidence:	Confirmed

Vulnerability 2 - Project Equalization Process:

<Affected packages: Operation Monitoring Basic Function>

On a computer where the affected package(s) of the affected product is installed, if a certain communication frame is transmitted to the process which equalizes the project data base with engineering function, a buffer overflow occurs and all the operation and monitoring functions in the computer are disabled. There is a potential risk that successful exploitation of this vulnerability allows remote attackers to execute arbitrary code.

CVSS Base Score: 9.0, Temporal Score: 7.8

Access Vector:	Network
Access Complexity:	Low
Authentication:	None
Confidentiality Impact (C):	Partial
Integrity Impact (I):	Partial
Availability Impact (A):	Complete
Exploitability:	High
Remediation Level:	Official Fix
Report Confidence:	Confirmed

Vulnerability 3 - Batch Management Process:

<Affected packages: Batch Management Package>

On a computer where the affected package(s) of the affected product is installed, if a certain communication frame is transmitted to the batch management process, a buffer overflow occurs and the batch management function is disabled. There is a potential risk that successful exploitation of this vulnerability allows remote attackers to execute arbitrary code.

CVSS Base Score: 8.3, Temporal Score: 6.9

Access Vector:	Network
Access Complexity:	Medium
Authentication:	None
Confidentiality Impact (C):	Partial
Integrity Impact (I):	Partial
Availability Impact (A):	Complete
Exploitability:	Functional
Remediation Level:	Official Fix
Report Confidence:	Confirmed

Vulnerability 4 - Simulator Management Process in the Expanded Test Functions:

<Affected Packages: Expanded Test Functions Package>

On a computer where the affected package(s) of the affected product is installed, if a certain communication frame is transmitted to the process which receives a request to FCS simulator Run/Quit from other PC, a buffer overflow occurs and the expanded test function is disabled. There is a potential risk that successful exploitation of this vulnerability allows remote attackers to execute arbitrary code.

CVSS Base Score: 8.3, Temporal Score: 6.9

Access Vector:	Network
Access Complexity:	Medium
Authentication:	None
Confidentiality Impact (C):	Partial
Integrity Impact (I):	Partial
Availability Impact (A):	Complete
Exploitability:	Functional
Remediation Level:	Official Fix
Report Confidence:	Confirmed

Countermeasures:

Yokogawa provides patch software for the latest revisions of the affected products. By installing the patch software, or updating the systems to the latest version of software, the vulnerabilities found this time are corrected. For details about individual countermeasures by the affected product, please refer to < Table 1: List of Products affected by Vulnerabilities and Countermeasures >.

- To activate the patch software, the computer needs to be rebooted.
- In case the system uses earlier versions of the software, than the ones for which the software patches are provided, please upgrade to the revisions/versions as mentioned in the table and then apply for the software patches.

When Yokogawa service personnel perform updating the revision and application the software patch, those charges are borne by the customer.

Yokogawa strongly suggests all customers to introduce appropriate security measures not only for the vulnerabilities identified but also to the overall systems.

* Contact Yokogawa supports & services when your system is difficult to update to the latest revision.

Acknowledgement:

Yokogawa thanks to the following organizations and persons for their support and cooperation in finding CENTUM CS 3000 vulnerabilities.

- Mr. Juan Vazquez of Rapid 7 Inc.
- Mr. Julian Vilas Diaz
- CERT/CC, NCCIC/ICS-CERT and JPCERT/CC

Supports and Services:

For questions related to this document or how to obtain the patch software, please contact Yokogawa service department or access the below URL for more details.
https://contact.yokogawa.com/cs/gw?c-id=000498

Table 1: List of Products affected by Vulnerabilities and Countermeasures

Products	Affected Revisions	Countermeasures (Patch software for the latest revision or the latest revision of products)
CENTUM CS 1000	All revisions	End of support (*1)
CENTUM CS 3000 CENTUM CS 3000 Entry Class	R2.23.00 or earlier	End of support (*1)
	R3.09.50 or earlier	Fixes vulnerabilities 1 to 4 in this document and vulnerability in YSAR-14-0002: Patch Software for R3.09.50 (R3.09.79) (*4)
CENTUM VP CENTUM VP Entry Class	R4.03.00 or earlier	Fixes vulnerabilities 1 to 4 in this document and vulnerability in YSAR-14-0002: Patch Software for R4.03.00 (R4.03.55) (*4)
	R5.03.20 or earlier	Fixes vulnerabilities 1 to 4 in this document and vulnerability in YSAR-14-0002: Patch Software for R5.03.20 (R5.03.51) (*4)
B/M9000CS	R5.05.01 or earlier	This product is not affected by the vulnerability; however, this product is affected by the existence of CENTUM CS 3000 or CS 1000 installed on the same PC. Follow these steps: - Update B/M9000CS to R5.05.01 - Update co-installed CENTUM CS 3000 to the latest revision(R3.09.50) - Apply patch software (R3.09.73) and (R3.09.75) * If CENTUM CS 1000 is installed in the system, consider migration to successor.
B/M9000 VP	R7.03.01 or earlier	This product is not affected by the vulnerability; however, this product is affected by the existence of CENTUM VP installed on the same PC. Follow these steps: - Update B/M9000 VP to R7.03.01 - Update co-installed CENTUM VP to the latest revision (R5.03.20) - Apply patch software (R5.03.38)
ProSafe-RS	R1.03.00 or earlier	Fixes vulnerability 1: Patch Software for R1.03.00 (R1.03.15)
	R2.03.80 or earlier	Fixes vulnerability 1: Patch Software for R2.03.80 (R2.03.89)
	R3.02.10 or earlier	Fixes vulnerability 1: Patch Software for R3.02.10 (R3.02.14)
ProSafe-RS (CHS2200: SOE OPC interface package)	R1.03.00 or earlier	Fixes vulnerability 1: Patch Software for R1.03.00 (R1.03.15)
	R2.03.80 or earlier	Fixes vulnerability 1: Patch Software for R2.03.80 (R2.03.89) and (R2.03.91)
	R3.02.10 or earlier	Fixes vulnerability 1: Patch Software for R3.02.10 (R3.02.14) and (R3.02.15)
Exaopc (Only Server)	R3.72.00 or earlier	Fixes vulnerabilities 1 to 4 in this document and vulnerability in YSAR-14-0002: Patch Software for R3.72.00 (R3.72.03) (*4)
Exapilot (Server / Client)	R3.96.00 or earlier	Fixes vulnerability 1: Patch Software for R3.96.00 (R3.96.01)
Exaplog (Server / Client)	R3.40.00 or earlier	Fixes vulnerability 1: Patch Software for R3.40.00 (R3.40.01)
Exaquantum (Only Server)	From R2.02.50 to R2.80.00	Fixes vulnerability 1: Latest Revision (R2.85.00) (*2)
Exaquantum/Batch (Only Server)	R2.50.10 or earlier	Fixes vulnerability 1: Patch Software for R2.50.10 (R2.50.18)
Exasmoc (Only Server)	R4.03.20 or earlier	Fixes vulnerability 1: Patch Software for R4.03.20 (R4.03.21)
Exarqe (Only Server)	R4.03.20 or earlier	Fixes vulnerability 1: Patch Software for R4.03.20 (R4.03.21)
AAASuite (Server / Client)	R1.20.13 or earlier	Patch software for Exapilot is applicable: Fixes vulnerability 1: Patch Software for R1.20.13 (Exapilot R3.95.04)
PRM	R3.11.20 or earlier	Fixes vulnerability 1: Patch Software for R3.11.20 (R3.11.24)
STARDOM FCN/FCJ OPC Server for	R3.40.01 or earlier	Fixes vulnerability 1: Patch Software for R3.40.01 (R3.40.03)

Windows (Only Server)		
Field Wireless Device OPC Server (Only Server)	R2.01.01 or earlier	Fixes vulnerability 1: Patch Software for R2.01.01 (R2.01.02)
DAQOPC DAQOPC for DARWIN	R3.01 or earlier	Contact above supports and services.
FieldMate	R1.03 or earlier	Contact above supports and services.
EJXMVTool	From R1.02.00 to R1.02.02	Contact above supports and services.
RPO Production Supervisor VP (Only Server)	R1.03.00 or earlier	Fixes vulnerability 1: Patch Software for R1.03.00 (R1.03.01)
CENTUM Long-term Trend Historian	All revisions	End of support (*1)
CENTUM Event Viewer Package	All revisions	End of support (*1)
OmegaLand/OPC server interface module	-	This product is not affected by the vulnerability; however, this product is affected by the existence of Exaopc installed on the same PC. Follow these steps: - Update co-installed Exaopc to the latest revision (R3.72.00) - Apply patch software (R3.72.01)

*1: Contact above supports and services for end of support products.
*2: In order to receive the latest revisions (including install media) of Exaopc and Exaquantum, an annual maintenance contract (AMC, standard plan) is required.
*3: Contact above supports and services when your system is difficult to update to the latest revision.
*4: Update patch software revision which include vulnerability described in YSAR-14-0002.

Reference:

1. A Complete Guide to the Common Vulnerability Scoring System (CVSS)
   http://www.first.org/cvss/cvss-guide.pdf
   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 users considering the security measures equipped with the overall systems.

2. ICS-CERT ADVISORY : ICSA-14-070-01
   http://ics-cert.us-cert.gov/advisories/ICSA-14-070-01

Revision History:

March 7, 2014	1st Edition
April 7, 2014	2nd Edition: CVSS base and temporal scores are added. Items 2 and 3 of the References are added.
May 9, 2014	3rd Edition: Vulnerability 4 is added. Information on the affected products other than CENTUM CS 3000 is added. Update information of Supports and Services.
July 7, 2014	4th Edition: Update patch software revision which include vulnerability described in YSAR-14-0002.
December 22, 2017	5th Edition: URL in Supports and Services is updated.

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