Yokogawa Security Advisory Report

YSAR-14-0002E
Published on July 7, 2014
Last updated on December 22, 2017

YSAR-14-0002E: Buffer Overflow Vulnerability in CENTUM systems and Exaopc

Overview:

A computer where CENTUM system or Exaopc is installed has been found with a buffer overflow vulnerability when Expanded Test Functions are in use. After the investigation, Yokogawa identified the range of products that could be influenced by the vulnerability and summarized the countermeasures 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 vulnerability reported in this document.
Any computer on which these products are installed has vulnerability.

CENTUM CS 1000, CENTUM CS 3000, CENTUM CS 3000 Entry Class,
CENTUM VP, CENTUM VP Entry Class,
Exaopc, B/M9000CS, B/M9000 VP

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

Vulnerability - Communication Simulation Process in the Expanded Test Functions:

<Affected Packages: Expanded Test Functions Package>
<Condition of occurrence: When Expanded Test Functions are in use>

On a computer where the affected package(s) of the affected product is installed, if an intentionally crafted packet is transmitted to the process which simulates control network communication while the expanded test functions being executed, a buffer overflow occurs and the expanded test functions are 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, 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	R2.23.00 or earlier	End of support (*1)
CENTUM CS 3000 Entry Class	R3.09.50 or earlier	Patch Software for R3.09.50 (R3.09.79)
CENTUM VP	R4.03.00 or earlier	Patch Software for R4.03.00 (R4.03.56)
CENTUM VP Entry Class	R5.03.20 or earlier	Patch Software for R5.03.20 (R5.03.51)
Exaopc (Only Server)	R3.72.00 or earlier	Patch Software for R3.72.00 (R3.72.03)
B/M9000CS	R5.05.01 or earlier	B/M software 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 (R3.09.79) * If CENTUM CS 1000 is installed in the system, consider migration to successor.
B/M9000 VP	R7.03.01 or earlier	B/M software 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 (R5.03.51)

*1: Contact above supports and services for end of support products.
*2: Contact above supports and services when your system is difficult to update to the latest revision.

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.

Revision History:

July 7, 2014 1st Edition
December 22, 2017 2nd Edition: URL in Supports and Services is updated.

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