Yokogawa Security Advisory Report

YSAR-14-0003E
Published on September 17, 2014
Last updated on December 22, 2017

YSAR-14-0003E: Arbitrary File Read/Write Vulnerability in CENTUM series and Exaopc

Overview:

A vulnerability has been found with CENTUM series installed with Batch Management Packages and Exaopc. The vulnerability allows arbitrary files to be read and written on computers running these software packages. 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 series with Batch Management Packages
  - CENTUM CS 3000 (R3.09.50 or earlier)
  - CENTUM CS 3000 Entry Class (R3.09.50 or earlier)
  - CENTUM VP (R4.03.00 or earlier, R5.04.00 or earlier)
  - CENTUM VP Entry Class (R4.03.00 or earlier, R5.04.00 or earlier)
- Exaopc (R3.72.10 or earlier)

Vulnerability - Batch Management Process (BKBCopyD.exe):

On a computer where the affected product(s) is installed, if a certain communication frame is transmitted to the process which manages batches (TCP port No.20111), arbitrary files accessible with the user rights on the drive where the affected product(s) is installed can be read and written.

CVSS Base Score: 6.8, Temporal Score: 5.6

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

When the system-wide network is properly managed (i.e., when the affected product(s) is/are on an isolated network), the risk of exploiting this vulnerability could be low.

Countermeasures:

Yokogawa will start providing patch software for the latest revisions of the affected products from the end of September. Please contact the supports and services in the following section for the detail date of release.

This patch software mitigates the risk of this vulnerability while ensuring the compatibility of communications for the batch managed function.

Meanwhile, until the release of the patch software, the risk of this vulnerability can be mitigated by implementing the mitigation measures described in the following section.

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.

Mitigation Measures:

If a network has a firewall, the risk of this vulnerability can be mitigated by configuring the following setting.

- Block external data communications from outside of the control system network on TCP port No.20111
- Allow internal traffic on TCP port No.20111 only between CENTUM systems with Batch Management Packages
- Block the traffic on TCP port No.20111 to Exaopc installations.

Yokogawa recommends that you properly manage your network to prevent suspicious devices from connecting to the network to which the affected product(s) is connected.

When Yokogawa service personnel perform firewall setup, those charges are borne by the customer.

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

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:

September 17, 2014 1st Edition
December 5, 2014 2nd Edition: Correct Affected Products.
December 22, 2017 3rd Edition: URL in Supports and Services is updated.

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