# Yokogawa Security Advisory Report

YSAR-18-0001

Published on January 22, 2018
Last updated on January 22, 2018

## YSAR-18-0001: Faked and blocked alarms Vulnerability in CENTUM and Exaopc

### Overview:

Faked and blocked alarms vulnerability have been found with message management function in CENTUM series and Exaopc. Yokogawa identified the range of products that could be impacted by the vulnerability in this document.
Review the document and confirm which products are affected in order to implement security measures for the overall systems. Also please consider applying the countermeasures as needed.

### Affected Products:

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

- CENTUM series
  - CENTUM CS 1000 (All Revisions)
  - CENTUM CS 3000 (R3.09.50 or earlier)
  - CENTUM CS 3000 Small (R3.09.50 or earlier)
  - CENTUM VP (R6.03.20 or earlier)
  - CENTUM VP Small (R6.03.20 or earlier)
  - CENTUM VP Basic (R6.03.20 or earlier)
- Exaopc (R3.75.00 or earlier)
- B/M9000CS (All Revisions)
- B/M9000 VP (R8.01.01 or earlier)

### Vulnerability:

If an attacker in some way managed to invade a computer on which a vulnerable product is installed, there is a risk that an attacker may be able to do the following attacks by exploiting the vulnerability of the message management function.

· Generating fake alarms
An attacker will be able to generate fake system alarms or process alarms for the message management service of the affected product.

· Blocking alarm notification
An attacker will be able to block displaying system alarms or process alarms that was supposed to display on the screen.

CVSS v2 Base Score: 5.9, Temporal Score: 4.6

| Access Vector (AV) | Local (L) | Adjacent Network (A) | Network (N) |
|---|---|---|---|
| Access Complexity (AC) | High (H) | Medium (M) | Low (L) |
| Authentication (Au) | Multiple (M) | Single (S) | None (N) |
| Confidentiality Impact (C) | None (N) | Partial (P) | Complete (C) |
| Integrity Impact (I) | None (N) | Partial (P) | Complete (C) |
| Availability Impact (A) | None (N) | Partial (P) | Complete (C) |

| | | | | | |
|---|---|---|---|---|---|
| Exploitability (E) | Unproven (U) | Proof-of-Concept(POC) | Functional (F) | High (H) | Not Defined (ND) |
| Remediation Level (RL) | Official Fix (OF) | Temporary Fix (TF) | Workaround (W) | Unavailable (U) | Not Defined (ND) |
| Report Confidence (RC) | Unconfirmed (UC) | Uncorroborated (UR) | Confirmed (C) | Not Defined (ND) | |

## Countermeasures:

By installing below patch software, or updating the systems to the latest version of software, the vulnerability found this time are corrected.

| Products | Affected Revisions | Countermeasures |
|---|---|---|
| CENTUM CS 1000 | All revisions | No patch software will be available because these products are already end of support.<br>Please consider migrating to latest CENTUM VP. |
| CENTUM CS 3000<br>CENTUM CS 3000 Small | R3.09.50 or earlier | |
| CENTUM VP<br>CENTUM VP Small<br>CENTUM VP Basic | R4.03.00 or earlier | |
| | R5.04.20 or earlier | Patch Software for R5.04.20 (R5.04.B2) |
| | R6.03.10 or earlier | has been remediated in R6.04.00 |
| Exaopc | R3.75.00 or earlier | has been remediated in R3.76.00 |
| B/M9000CS | All revisions | 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. |
| B/M9000 VP | R8.01.01 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.<br>If installed CENTUM VP need to update, also please update B/M9000 VP to suitable revision. |

When Yokogawa service personnel perform system upgrade or install patches, those charges are borne by the customer.

If it is inconvenient to upgrade to latest recommended versions above, then it is possible to minimize the risk of this vulnerability by applying the actions outlined in the next section.

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

## Mitigation Measures:

Direct attacks by exploiting this vulnerability via a network cannot be done. Therefore, the risk of this vulnerability being exploited can be reduced by preventing attackers from invading computers by applying the following anti-malware measures (security measures) on computers on which vulnerable products are installed.

- Install Anti-malware software.
- Install White Listing software.
- Apply mitigation measures for malware entry route via removable media such as a USB memory stick.

Please consider applying Yokogawa Endpoint Security Service for above malware countermeasures.

## Supports:

For questions related to this document, please contact the below.
https://contact.yokogawa.com/cs/gw?c-id=000498

## Reference:

1. A Complete Guide to the Common Vulnerability Scoring System (CVSS)
   https://www.first.org/cvss/cvss-v2-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 document 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:

January 22, 2018 1st Edition

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