# *Yokogawa Security Advisory Report*

YSAR-19-0001

| | |
|---|---|
| Published on | January 25, 2019 |
| Last updated on | February 28, 2019 |

## YSAR-19-0001: Vulnerability of access control in License Manager Service of Yokogawa products

### Overview:

A vulnerability of access control has been found in License Manager Service of Yokogawa products. Yokogawa identified the range of products that could be impacted by the vulnerability in this report.

Review the report and confirm which products are affected to implement security measures for the overall systems. Also, please consider applying the countermeasures as needed.

### Affected Products:

Following are the products that would be affected by the vulnerability.

| | |
|---|---|
| • CENTUM | |
| CENTUM VP | (R5.01.00 - R6.06.00) |
| CENTUM VP Entry Class | (R5.01.00 - R6.06.00) |
| • ProSafe-RS | (R3.01.00 - R4.04.00) |
| • PRM | (R4.01.00 - R4.02.00) |
| • B/M9000 VP | (R7.01.01 - R8.02.03) |

### Vulnerability:

This vulnerability may allow remote attackers to create / override any files on anywhere with user privilege on computer which License Manager Service runs. (This vulnerability cannot create/remove folder, cannot remove file, cannot execute command/file.)
There is a potential risk that if remote attackers use this vulnerability, they can hinder the functions of that computer, etc.

CVSS v3 Base Score: 8.1, Temporal Score: 7.3
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

## Countermeasures:

By applying the patch, the vulnerability is corrected.

| Products | Affected Revisions | Countermeasures |
|---|---|---|
| CENTUM VP<br>CENTUM VP Entry Class | R5.01.00 - R5.04.00 | Please consider revision up to R5.04.20 and applying patch software for R5.04.20 (R5.04.C5). |
| | R5.04.20 | Please apply patch software for R5.04.20 (R5.04.C5). |
| | R6.01.00 - R6.05.00 | Please consider revision up to R6.06.00 and applying patch software for R6.06.00 (R6.06.03). |
| | R6.06.00 | Please apply patch software for R6.06.00 (R6.06.03). |
| ProSafe-RS | R3.01.00 - R3.02.10 | Please consider revision up to R3.02.20 and applying patch software for R3.02.20 (R3.02.38). |
| | R3.02.20 | Please apply patch software for R3.02.20 (R3.02.38). |
| | R4.01.00 - R4.03.10 | Please consider revision up to R4.04.00 and applying patch software for R4.04.00 (R4.04.01). |
| | R4.04.00 | Please apply patch software for R4.04.00 (R4.04.01). |
| PRM | R4.01.00 | Please consider revision up to R4.02.00 and applying patch software for R4.02.00 (R4.02.01). |
| | R4.02.00 | Please apply patch software for R4.02.00 (R4.02.01). |
| B/M9000 VP | R7.01.01 - R8.02.03 | 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 revision up or install patches, those charges are borne by the customer.
Yokogawa strongly suggests all customers to introduce appropriate security measures not only for the vulnerability identified but also to the overall systems.

## Supports:

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

## 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 has to be judged by the users considering the security measures equipped with the overall systems.

## ACKNOWLEDGMENTS:

Yokogawa sincerely thanks the following party.

- Segey Temnikov, Kaspersky Lab ICS CERT

## Revision History:

| | |
|---|---|
| January 25, 2019 | 1st Edition |
| February 28, 2019 | Updated "Vulnerability" |

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