Yokogawa Security Advisory Report

YSAR-18-0008
Published on December 21, 2018
Last updated on December 21, 2018

YSAR-18-0008: Denial of Service (DoS) vulnerability in Vnet/IP Open Communication Driver

Overview:

A vulnerability has been found in Vnet/IP Open Communication Driver. 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 CS 3000 (R3.05.00 - R3.09.50)
  - CENTUM CS 3000 Entry Class (R3.05.00 - R3.09.50)
  - CENTUM VP (R4.01.00 - R6.03.10)
  - CENTUM VP Entry Class (R4.01.00 - R6.03.10)
- Exaopc (R3.10.00 - R3.75.00)
- PRM (R2.06.00 - R3.31.00)
- ProSafe-RS (R1.02.00 - R4.02.00)
- FAST/TOOLS (R9.02.00 - R10.02.00)
- B/M9000 VP (R6.03.01 - R8.01.90)

Vulnerability:

This vulnerability may allow an attacker to stop communication function of Vnet/IP Open Communication Driver by DoS attack.

CVSS v3 Base Score: 7.5, Temporal Score: 7.2
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C

Countermeasures:

By updating to the latest version or applying the patch, the vulnerability is corrected.

Products	Affected Revisions	Countermeasures
CENTUM CS 3000 CENTUM CS 3000 Entry Class	R3.05.00 - R3.09.50	No patch software will be available because these products are already end of support. Please consider system upgrade to latest CENTUM VP.
CENTUM VP CENTUM VP Entry Class	All revisions of R4 series	
	All revisions of R5 series	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08.
	R6.03.10 or earlier in R6 series	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08. This vulnerability has been fixed in R6.04.00.
Exaopc	R3.10.00 - R3.60.00	No patch software will be available because these products are already end of support. Please consider system upgrade to latest version/revision.
	R3.70.00 - R3.75.00	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08. This vulnerability has been fixed in R3.76.00.
PRM	R2.06.00 - R3.04.00	No patch software will be available because these products are already end of support. Please consider system upgrade to latest version/revision.
	R3.05.00 - R3.31.00	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08. This vulnerability has been fixed in R4.01.00.
ProSafe-RS	All revisions of R1, R2 series	No patch software will be available because these products are already end of support. Please consider system upgrade to latest version/revision.
	All revisions of R3 series	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08.
	R4.02.00 or earlier in R4 series	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08. This vulnerability has been fixed in R4.03.00
FAST/TOOLS	R9.02.00 - R9.03.00	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08.
	R9.04.00 - R9.05.00	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08.
	R10.02.00 or earlier in R10 series	Please apply Vnet/IP Open Communication Driver patch software for R10.01.08. This vulnerability has been fixed in R10.03.00.
B/M9000CS	-	This product is not affected by the vulnerability. CENTUM CS 3000 installed with this product is not available for Vnet/IP.
B/M9000 VP	R6.03.01 - R8.01.90	This product is not affected by the vulnerability. However, this product is affected by the existence of CENTUM VP installed on the same PC. 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.
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.

Revision History:

December 21, 2018 1st Edition

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