Yokogawa Security Advisory Report

YSAR-26-0002

Published on February 13, 2026
Last updated on February 13, 2026

YSAR-26-0002: Vulnerabilities in Vnet/IP Interface Package

Overview:
Vulnerabilities have been found in Vnet/IP Interface Package. Yokogawa has identified the range of affected products in this report.
Please review the report and confirm which products are affected to implement security measures for the overall systems. Please consider applying the countermeasures as needed.

Affected Products:
This vulnerability affects the following products.

Product name	Affected Versions	Yokogawa products related to affected products (*2)
Vnet/IP Interface Package (*1) (for CENTUM VP R6 VP6C3300) (for CENTUM VP R7 VP7C3300)	R1.07.00 or earlier	CENTUM VP R6, CENTUM VP R7,

*1: Vnet/IP Interface Package is a product required for Yokogawa products on a Virtualization Platform to communicate via Vnet/IP.
*2: If those products are deployed on a Virtualization Platform and affected products are installed, it will be impacted by the vulnerabilities described in this report.

Vulnerability 1:
If affected product receive maliciously crafted packets, a DoS attack may cause Vnet/IP communication functions to stop or arbitrary programs to be executed.

CWE-787 : Out-of-bounds Write
CWE-191 : Integer Underflow
CVE: CVE-2025-1924
CVSS v3 Base score: 6.9
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:H
CVSS v4 Base score: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:H/SC:N/SI:L/SA:L

Vulnerability 2:
If affected product receive maliciously crafted packets, Vnet/IP software stack process may be terminated.

CWE-617 : Reachable Assertion
CVE: CVE-2025-48019
CVSS v3 Base score: 5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 Base score: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-617 : Reachable Assertion
CVE: CVE-2025-48020
CVSS v3 Base score: 5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 Base score: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-191 : Integer Underflow
CVE: CVE-2025-48021
CVSS v3 Base score: 5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 Base score: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-130 : Improper Handling of Length Parameter Inconsistency
CVE: CVE-2025-48022
CVSS v3 Base score: 5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 Base score: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-617 : Reachable Assertion
CVE: CVE-2025-48023
CVSS v3 Base score: 5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 Base score: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Countermeasures:

	Affected Revisions	Fixed Revision	Countermeasures
Vnet/IP Interface Package	R1.07.00 or earlier	R1.08.00	Please apply patch software (R1.08.00).

 # Regarding the vulnerabilities described in this report
The vulnerabilities described in this report do not constitute non-conformities of the affected products. Therefore, if a customer requests Yokogawa to perform work related to the countermeasures described in this report, the associated costs will be borne by the customer.

 # Recommendation for countermeasures
To help reduce cybersecurity risks, Yokogawa recommends applying the countermeasures described in this report.
However, the actual impact of the vulnerabilities described in this report may vary depending on each customer's system environment. We recommend that customers carefully review this report and determine whether and when to apply the countermeasures based on a risk assessment of their system environment.

Yokogawa offers support for applying the countermeasures described in this report, as well as assistance with other cybersecurity measures. Please contact your local Yokogawa supporting office for further information or support.

Supports:

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

Acknowledgement:

The vulnerabilities were discovered and notified by the following organizations and persons.

- Dmitry Sklyar (Positive Technologies) for CVE-IDs: CVE-2025-1924, CVE-2025-48019, CVE-2025-48020, CVE-2025-48023
- Demid Uzenkov (Positive Technologies) for CVE-IDs: CVE-2025-1924, CVE-2025-48021, CVE-2025-48022

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:

February 13, 2026: 1st Edition

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