Yokogawa Security Advisory Report

YSAR-22-0005

Published on June 3, 2022
Last updated on July 27, 2022

YSAR-22-0005: Denial of Service (DoS) vulnerability in Wide Area Communication Router

Overview:
A vulnerability has been found in Wide Area Communication Router (WAC Router). Yokogawa has identified the range of affected products in this report.
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:
• Communication Module for Wide Area Communication Router (for AW810D) VI461
Affected Revisions: Vnet/IP firmware (F) R12 or earlier

Vulnerability:
If WAC Router is subjected to a DoS attack with malformed packets, the functions provided by WAC Router may stop.

Use of Insufficiently Random Values (CWE-330)
CVE: CVE-2022-32284
CVSS v3 Base score: 5.9
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Countermeasures:
Communication Module for Wide Area Communication Router (for AW810D) VI461

Affected Revisions	Fixed Revision	Countermeasures
Vnet/IP firmware (F) R12 or earlier	R13	Please update to R13 or later.

Yokogawa recommends updating as above the countermeasures.
Vnet/IP firmware cannot be updated by the customer.
If the customer wishes to update, please ask our sales or service staff to update Vnet/IP firmware.
Update charges are borne by the customer.

Yokogawa strongly recommends all customers to establish and maintain a full security program, not only for the vulnerability identified in this YSAR. Security program components are: Patch updates, Anti-virus, Backup and recovery, zoning, hardening, whitelisting, firewall, etc. Yokogawa can assist in setting up and running the security program continuously. For considering the most effective risk mitigation plan, as a starting point, Yokogawa can perform a security risk assessment.

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

Revision History:

June 3, 2022: 1st Edition
July 27, 2022: 2nd Edition: Added CVE

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