Yokogawa Security Advisory Report

YSAR-22-0008

Published on July 29, 2022
Last updated on July 29, 2022

YSAR-22-0008: Denial of Service (DoS) vulnerability in CENTUM controller FCS

Overview:

Denial of Service (DoS) vulnerability has been found in CENTUM controller FCS. 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:

- CENTUM VP / CS 3000 controller FCS
  - CP31, CP33, CP345
  - CP401, CP451

For details of their revisions, please see below Countermeasures.

Vulnerability:

If CENTUM VP / CS 3000 controller FCS is subjected to a Denial of Service (DoS) attack with malformed packets, ADL communication may stop.

Resource Management Errors (CWE-399)
CVE: CVE-2022-33939
CVSS v3 Base score: 6.5
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Countermeasures:

CENTUM VP / CS 3000 controller FCS
・CP31, CP33, CP345

	Affected Revisions	Countermeasures
CENTUM CS 3000 CENTUM CS 3000 Entry Class	All Revision	No patch software will be available because these products are already end of support. Please consider system upgrade to the latest revision of CENTUM VP.

・CP401, CP451

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM CS 3000 CENTUM CS 3000 Entry Class	All Revision	-	No patch software will be available because these products are already end of support. Please consider system upgrade to the latest revision of CENTUM VP.
CENTUM VP CENTUM VP Entry Class	R4.01.00 - R4.03.00	-	
	R5.01.00 - R5.04.20	R5.04.78	Please update to R5.04.20 and apply Patch Software for R5.04.20 (R5.04.78).
	R6.01.00 - R6.03.00	R6.03.10	Please update to R6.03.10 or later.

Yokogawa recommends updating as above the countermeasures. When Yokogawa service personnel perform update, those 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:

July 29, 2022: 1st Edition

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