Yokogawa Security Advisory Report

YSAR-24-0003
Published on September 17, 2024
Last updated on September 17, 2024

YSAR-24-0003: Denial of Service (DoS) vulnerability in Dual-redundant Platform for Computer

Overview:
A Denial of Service (DoS) vulnerability has been found in Dual-redundant Platform for Computer.
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 Revisions
Dual-redundant Platform for Computer (PC2CKM)	R1.01.00 - R2.03.00

Vulnerability:
If a computer on which the affected product is installed receives a large number of UDP broadcast packets in a short period, occasionally that computer may restart.
If both the active and standby computers are restarted at the same time, the functionality on that computer may be temporarily unavailable.

CWE-252 : Unchecked Return Value
CVE: CVE-2024-8110
CVSS v3 Base score: 7.5
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Countermeasures:

	Affected Revisions	Fixed Revision	Countermeasures
Dual-redundant Platform for Computer	R1.01.00 - R2.03.00	R2.03.10	Please update to the R2.03.10.

Yokogawa recommends updating as described in the above 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 has to be judged by the users considering the security measures equipped with the overall systems.

Revision History:

September 17, 2024: 1st Edition

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