Yokogawa Security Advisory Report

YSAR-21-0002

Published on April 23, 2021
Last updated on April 23, 2021

YSAR-21-0002: Affected Yokogawa products by CPU Vulnerability Meltdown / Spectre

Overview:

Yokogawa products that are affected by CPU Vulnerability as known Meltdown / Spectre have been found. 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 Controller FCS

FCS processor modules	FCS Type
CP461	AFV30S, AFV30D, AFV40S, AFV40D, A2FV50S, A2FV50D, A2FV70S, A2FV70D

Vulnerability:

Please refer to the below note regarding the vulnerabilities.
"Vulnerability Note VU#584653 CPU hardware vulnerable to side-channel attacks"
https://www.kb.cert.org/vuls/id/584653

Countermeasures:

• CENTUM VP Controller FCS

FCS processor modules	Countermeasures
CP461	・Please update to CENTUM VP R6.08.00 or later. ・OR, Please replace to CP471 which is not affected by this vulnerability.

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.

Patching is by far the best protection against this vulnerability being exploited, but if for example for operational reason, patching is not possible. Yokogawa specialist can consult on the best course of action.

Supports:

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

Revision History:

April 23, 2021: 1st Edition

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