Yokogawa Security Advisory Report

YSAR-21-0003

Published on May 31, 2021
Last updated on October 14, 2021

YSAR-21-0003: Affected Yokogawa products by Treck IP Stack vulnerabilities

Overview:

Yokogawa products that are affected by Treck IP Stack vulnerabilities as known Ripple20 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:

- YFGW410, YFGW510, YFGW520

- CENTUM VP Controller FCS

FCS processor modules	FCS Type
CP451	AFV10S, AFV10D
CP461, CP471	AFV30S, AFV30D, AFV40S, AFV40D, A2FV50S, A2FV50D, A2FV70S, A2FV70D

- ProSafe-RS Controller SCS

SCS processor modules	SCS Type
SCP451	SSC50S, SSC50D, SSC57S, SSC57D
SCP461, S2CP471	SSC60S, SSC60D, S2SC70S, S2SC70D
L1CP471	L1SC70S, L1SC70D

- Yokogawa products that installed Vnet/IP Interface Card (VI701, VI702) *1 *2
  *1 CENTUM VP, CENTUM CS 3000, ProSafe-RS, Exaopc, PRM, FAST/TOOLS, B/M9000 VP etc.
  *2 Vnet/IP Interface Package (VP6C3300, RS4C3300, PM4C3300, NTPF330) that used with IA System Products Virtualization Platform, Dual-redundant Platform for Computer (FT2SDR01, PC2CKM) are not affected by this vulnerabilities.

- Communication Module for V net Router (for AVR10D) VI451
- Communication Module for Wide Area Communication Router (for AW810D) VI461

Vulnerability:

Please refer to the ICS Advisory (ICSA-20-168-01) regarding the vulnerabilities.
https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01

About YFGW410, YFGW510, YFGW520

- The vulnerabilities affect the wired interfaces of these products. The vulnerabilities may allow a remote attacker to prevent communication with the field wireless backbone in these products.
- Regarding YFGW410, the field wireless backbone interfaces of are affected. The field network interfaces are not affected.

About CENTUM VP Controller FCS, ProSafe-RS Controller SCS,
Yokogawa products that installed Vnet/IP Interface Card (VI701, VI702),
Communication Module for V net Router, Communication Module for Wide Area Communication Router

- The vulnerabilities affect the Vnet/IP firmware of these products. If attacked using this vulnerability, the module on these products may be stop (In the case of duplexed station, Control switch over or the standby module failure) or the communication capability of Vnet/IP may be reduced.

Countermeasures:

Products	Affected Revisions	Fixed Revision	Countermeasures
YFGW410	R3.01.02 or earlier	R3.01.03	Please update to R3.01.03 or later.
YFGW510	R1.07.01 or earlier	R1.07.03	Please update to R1.07.03 or later
YFGW520	R2.01.01 or earlier	R2.01.03	Please update to R2.01.03 or later.

About YFGW410, YFGW510, YFGW520

- Customers can reduce cybersecurity risk of the vulnerabilities by not connecting these products to untrusted network and devices.

CENTUM VP Controller FCS

FCS processor modules	FCS Type	Affected Revisions	Fixed Revision	Countermeasures
CP451	AFV10S, AFV10D	Vnet/IP firmware (F1) R31 or earlier	R33	Please update to R33 or later.
CP461, CP471	AFV30S, AFV30D, AFV40S, AFV40D, A2FV50S, A2FV50D, A2FV70S, A2FV70D			

ProSafe-RS Controller SCS

SCS processor modules	SCS Type	Affected Revisions	Fixed Revision	Countermeasures
SCP451	SSC50S, SSC50D, SSC57S, SSC57D	Vnet/IP firmware (F1) R31 or earlier	R33	Please update to R33 or later.
SCP461, S2CP471	SSC60S, SSC60D, S2SC70S, S2SC70D		R32	Please update to R32 or later.
L1CP471	L1SC70S, L1SC70D			

Yokogawa products that installed Vnet/IP Interface Card (VI701, VI702)

Affected Revisions	Fixed Revision	Countermeasures
Vnet/IP firmware (F) R31 or earlier	R33	Please update to R33 or later.

Communication Module for V net Router (for AVR10D) VI451

Affected Revisions	Fixed Revision	Countermeasures
Vnet/IP firmware (F2) R31 or earlier	R33	Please update to R33 or later.

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

Affected Revisions	Fixed Revision	Countermeasures
Vnet/IP firmware (F) R11 or earlier	R12	Please update to R12 or later.

Yokogawa recommends updating as above the countermeasures. When Yokogawa service personnel perform update, those charges are borne by the customer.
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.

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

Revision History:

May 31, 2021: 1st Edition
September 23, 2021: Added several products in “Affected Products” and “Countermeasures”
October 14, 2021: Fix countermeasure of SCP451
* Contents of this report are subject to change without notice.