Yokogawa Security Advisory Report

YSAR-22-0009

Published on August 26, 2022
Last updated on August 26, 2022

YSAR-22-0009: Vulnerability in STARDOM controller

Overview:

A vulnerability has been found in STARDOM controller. 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:

- STARDOM FCN/FCJ R1.01 - R4.31

Vulnerability:

Please refer to the following ICS Advisory regarding the vulnerability of the module which is used in the above Affected Products.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-172-04

Countermeasures:

Please apply the following mitigations.

- Enable packet filtering functionality*1 of the FCN/FCJ controller to only allow connection from trusted hosts.
- Enable Project Protection*2 of Resource Configurator to not allow download a project file from Logic Designer to the controller.

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.

*1 Revision up FCN/FCJ basic software to R4.20 or later for using the function. When Yokogawa service personnel perform revision up, those charges are borne by the customer.

*2 Revision up FCN/FCJ basic software to R4.02 or later for using the function. When Yokogawa service personnel perform revision up, those charges are borne by the customer.

Supports:

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

Acknowledgement:

The vulnerabilities were discovered and notified by the following organizations and persons.

- Jos Wetzels, Forescout

Revision History:
August 26, 2022: 1st Edition
* Contents of this report are subject to change without notice.