Yokogawa Security Advisory Report

YSAR-22-0002

Published on January 14, 2022
Last updated on March 25, 2022

YSAR-22-0002: Vulnerability of license function in Yokogawa products

Overview:

A vulnerability has been found in a module that is used in license function of Yokogawa products.
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:

- iDefine for ProSafe-RS R1.16.1 - R1.16.5 *1
- STARDOM FCN/FCJ Simulator R1.01 - R4.20 *2
- STARDOM VDS R4.01 - R7.50

*1 Dongle Gateway R1.0.0.0 which is supported in iDefine R1.16.4 is also affected. Dongle Gateway is a software that iDefine's customers can download on the Yokogawa Partner Portal Site the same as iDefine for ProSafe-RS.

*2 Only STARDOM FCN/FCJ Simulator option package is affected by this vulnerability.

Vulnerability:

Please refer to the following ICS Advisory regarding the vulnerability of the module which is used in the above Affected Products.
https://www.us-cert.gov/ics/advisories/icsa-19-339-01

Countermeasures:

Products	Affected Revisions	Fixed revision	Countermeasures
iDefine for ProSafe-RS (Dongle Gateway)	R1.16.1 - R1.16.5 (R1.0.0.0)	R1.16.6 (R1.0.2.0)	Please update to R1.16.6 or later. (Dongle Gateway: R1.0.2.0 or later)
STARDOM FCN/FCJ Simulator	R1.01 - R4.20	R4.30.01	Please update to R4.30.01 or later.
STARDOM VDS	R4.01 - R7.50	R8.01	Please update to R8.01 or later.

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:
January 14, 2022: 1st Edition
March 25, 2022: Added STARDOM VDS in “Affected Products” and “Countermeasures”, Updated STARDOM FCN/FCJ
* Contents of this report are subject to change without notice.