Yokogawa Security Advisory Report

YSAR-22-0007

Published on June 21, 2022
Last updated on June 29, 2022

YSAR-22-0007: Vulnerabilities in STARDOM

Overview:

Vulnerabilities have been found in STARDOM. 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:

Vulnerability 1:
- STARDOM FCN/FCJ R1.01 - R4.31

Vulnerability 2:
- STARDOM FCN/FCJ R4.10 - R4.31

Vulnerability 1:

This vulnerability may allow to an attacker to sniff network traffic with the FCN/FCJ controller. An attacker could read/change configuration or update tampered firmware to the controller by exploitation of this vulnerability.

- Cleartext Transmission of Sensitive Information (CWE-319)

CVE-2022-29519
CVSS v3 Base score: 4.8
CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N

Vulnerability 2:

This vulnerability may allow to an attacker to obtain hard-coded credentials. An attacker could read/change configuration or update tampered firmware to the controller by exploitation of this vulnerability. *

* An attacker could access to only the environment of FCN/FCJ CPU module dual-redundant by using hard-coded credentials.
(An attacker cannot access to the controller of single CPU configuration.)

- Use of Hard-coded Credentials (CWE-798)

CVE-2022-30997
CVSS v3 Base score: 6.3
CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H

Countermeasures:

Countermeasure for Vulnerability 1 and 2
Please apply the following mitigations.
- By using the packet filter function* of the FCN/FCJ controller, only allow connection from trusted hosts.
- Take measures against the network so that an attacker cannot capture network traffic.

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.

* 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.

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

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 have to be judged by the users considering the security measures equipped with the overall systems.

Revision History:

June 21, 2022: 1st Edition
June 29, 2022: Updated “Countermeasures”
* Contents of this report are subject to change without notice.