Yokogawa Security Advisory Report

YSAR-23-0003
Published on December 1, 2023
Last updated on December 1, 2023

YSAR-23-0003: Denial-of-Service Vulnerability in STARDOM

Overview:
A denial-of-service (DoS) vulnerability has 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:
- STARDOM FCN/FCJ R1.01 - R4.31

Vulnerability:
This vulnerability may allow to a remote attacker to cause a denial-of-service condition to the FCN/FCJ controller by sending a crafted packet. While sending the packet, the maintenance homepage of the controller could not be accessed. Therefore, functions of the maintenance homepage, changing configuration, viewing logs, etc. are not available. But the controller's operation is not stopped by the condition.

- Uncontrolled Resource Consumption (CWE-400)

CVE-2023-5915
CVSS v3 Base score: 5.3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Countermeasures:
Please apply the following mitigations. A patch software for the vulnerability is not provided.
- 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 send a malicious packet.

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.

- Roman Ezhov, Kaspersky

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:

December 1, 2023: 1st Edition
* Contents of this report are subject to change without notice.