Yokogawa Security Advisory Report

YSAR-18-0004

Published on May 21, 2018
Last updated on May 21, 2018

YSAR-18-0004: Vulnerability of hardcoded password in STARDOM controllers

Overview:

Vulnerability of hardcoded password has been found in STARDOM controllers. Yokogawa identified the range of products that could be impacted by the vulnerability in this report.

Review the report and confirm which products are affected to implement security measures for the overall systems. Also, please consider applying the countermeasures as needed.

Affected Products:

Following are the products that would be affected by this vulnerability.

- STARDOM controllers
  FCJ (R4.02 or earlier)
  FCN-100 (R4.02 or earlier)
  FCN-RTU (R4.02 or earlier)
  FCN-500 (R4.02 or earlier)

Vulnerability:

Affected products have hardcoded account and password. There is a risk that an attacker may login a controller with hardcoded account and the attacker may execute system commands.

CVSS v2 Base Score: 9.3, Temporal Score: 7.7

Access Vector (AV)	Local (L)	Adjacent Network (A)	Network (N)
Access Complexity (AC)	High (H)	Medium (M)	Low (L)
Authentication (Au)	Multiple (M)	Single (S)	None (N)
Confidentiality Impact (C)	None (N)	Partial (P)	Complete (C)
Integrity Impact (I)	None (N)	Partial (P)	Complete (C)
Availability Impact (A)	None (N)	Partial (P)	Complete (C)

Exploitability (E)	Unproven (U)	Proof-of-Concept(POC)	Functional (F)	High (H)	Not Defined (ND)
Remediation Level (RL)	Official Fix (OF)	Temporary Fix (TF)	Workaround (W)	Unavailable (U)	Not Defined (ND)
Report Confidence (RC)	Unconfirmed (UC)	Uncorroborated (UR)	Confirmed (C)	Not Defined (ND)	

Countermeasures:

By revision upgrading the FCN/FCJ basic software to R4.10 or later, the vulnerability found this time is corrected.

When Yokogawa service personnel perform system upgrade or install patches, those charges are borne by the customer.
Yokogawa strongly suggests all customers to introduce appropriate security measures not only for the vulnerability identified but also to the overall systems.

Supports:

For questions related to this report, please contact the below.
http://stardom.biz/

Reference:

1. A Complete Guide to the Common Vulnerability Scoring System (CVSS)
   http://www.first.org/cvss/cvss-v2-guide.pdf
   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 has to be judged by the users considering the security measures equipped with the overall systems.

Revision History:

May 21, 2018 1st Edition

* Contents of this report are subject to change without notice.