Yokogawa Security Advisory Report

YSAR-16-0002
Published on September 14, 2016
Last updated on September 14, 2016

YSAR-16-0002: Arbitrary command execution vulnerability in STARDOM

Overview:

STARDOM controller and Logic Designer do not require authentication to connect, which may allow attackers to execute arbitrary commands. 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 in order 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 FCN/FCJ (from R1.01 to R4.01)

Vulnerability:

Logic Designer can connect to STARDOM controller without authentication, then there is a risk that attackers may execute command such as stop application program, change values, and modify application.

CVSS v2 Base Score: 7.5, Temporal Score: 6.2

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:

The vulnerability has been remediated with the latest release R4.02. Please contact the supports in the following section on how to update.

Yokogawa strongly suggests all customers to introduce appropriate security measures not only for the vulnerabilities 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:

September 14, 2016 1st Edition

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