Yokogawa Security Advisory Report

YSAR-18-0007
Published on September 28, 2018
Last updated on September 28, 2018

YSAR-18-0007: Vulnerabilities in STARDOM controllers

Overview:

Vulnerabilities have been found in STARDOM controllers. Yokogawa identified the range of products that could be impacted by the vulnerabilities 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 these vulnerabilities.

● FCN-500	(R4.10 or earlier)
● FCN-RTU	(R4.10 or earlier)
● FCN-100, FCJ	(R4.10 or earlier)

Vulnerability:

The below vulnerabilities have been found in STARDOM controllers.

1. Vulnerability of credential management
   This vulnerability may allow an attacker to obtain credential for remote access to controllers.

   CVSS v3 Base Score: 9.4, Temporal Score: 8.6

Attack Vector (AV)	Physical (P)	Local (L)	Adjacent (A)	Network (N)
Attack Complexity (AC)	High(H)	Low(L)		
Privileges Required (PR)	High(H)	Low(L)	None(N)	
User Interaction (UI)	Required(R)	None(N)		
Scope (S)	Unchanged(U)	Changed(C)		
Confidentiality Impact (C)	None(N)	Low(L)	High(H)	
Integrity Impact (I)	None(N)	Low(L)	High(H)	
Availability Impact (A)	None(N)	Low(L)	High(H)	

Exploit Code Maturity (E)	Unproven (U)	Proof-of-Concept(P)	Functional (F)	High (H)	Not Defined (X)
Remediation Level (RL)	Official Fix (O)	Temporary Fix (T)	Workaround (W)	Unavailable (U)	Not Defined (X)
Report Confidence (RC)	Unknown(U)	Reasonable(R)	Confirmed (C)	Not Defined (X)	

2. Denial of service vulnerability to remote management function
   This vulnerability may allow an attacker to prevent access to remote management function of controllers.

CVSS v3 Base Score: 5.3, Temporal Score: 5.2

Attack Vector (AV)	Physical (P)	Local (L)	Adjacent (A)	Network (N)
Attack Complexity (AC)	High(H)	Low(L)		
Privileges Required (PR)	High(H)	Low(L)	None(N)	
User Interaction (UI)	Required(R)	None(N)		
Scope (S)	Unchanged(U)	Changed(C)		
Confidentiality Impact (C)	None(N)	Low(L)	High(H)	
Integrity Impact (I)	None(N)	Low(L)	High(H)	
Availability Impact (A)	None(N)	Low(L)	High(H)	

Exploit Code Maturity (E)	Unproven (U)	Proof-of-Concept(P)	Functional (F)	High (H)	Not Defined (X)
Remediation Level (RL)	Official Fix (O)	Temporary Fix (T)	Workaround (W)	Unavailable (U)	Not Defined (X)
Report Confidence (RC)	Unknown(U)	Reasonable(R)	Confirmed (C)	Not Defined (X)	

3. Hardcoded credential vulnerability of maintenance function
   This vulnerability may allow an attacker to log in to the controller's maintenance function and get information or be tampered. This attack can be executed only during maintenance work.

CVSS v3 Base Score: 8.3, Temporal Score: 7.9

Attack Vector (AV)	Physical (P)	Local (L)	Adjacent (A)	Network (N)
Attack Complexity (AC)	High(H)	Low(L)		
Privileges Required (PR)	High(H)	Low(L)	None(N)	
User Interaction (UI)	Required(R)	None(N)		
Scope (S)	Unchanged(U)	Changed(C)		
Confidentiality Impact (C)	None(N)	Low(L)	High(H)	
Integrity Impact (I)	None(N)	Low(L)	High(H)	
Availability Impact (A)	None(N)	Low(L)	High(H)	

Exploit Code Maturity (E)	Unproven (U)	Proof-of-Concept(P)	Functional (F)	High (H)	Not Defined (X)
Remediation Level (RL)	Official Fix (O)	Temporary Fix (T)	Workaround (W)	Unavailable (U)	Not Defined (X)
Report Confidence (RC)	Unknown(U)	Reasonable(R)	Confirmed (C)	Not Defined (X)	

4. Memory exhaustion vulnerability by not permitted request
   This vulnerability may allow an attacker to cause memory exhaustion by not permitted request to HTTP service of controllers.

CVSS v3 Base Score: 5.3, Temporal Score: 4.9

Attack Vector (AV)	Physical (P)	Local (L)	Adjacent (A)	Network (N)
Attack Complexity (AC)	High(H)	Low(L)		
Privileges Required (PR)	High(H)	Low(L)	None(N)	
User Interaction (UI)	Required(R)	None(N)		
Scope (S)	Unchanged(U)	Changed(C)		
Confidentiality Impact (C)	None(N)	Low(L)	High(H)	
Integrity Impact (I)	None(N)	Low(L)	High(H)	
Availability Impact (A)	None(N)	Low(L)	High(H)	

Exploit Code Maturity (E)	Unproven (U)	Proof-of-Concept(P)	Functional (F)	High (H)	Not Defined (X)
Remediation Level (RL)	Official Fix (O)	Temporary Fix (T)	Workaround (W)	Unavailable (U)	Not Defined (X)
Report Confidence (RC)	Unknown(U)	Reasonable(R)	Confirmed (C)	Not Defined (X)	

Countermeasures:

Revision up FCN/FCJ basic software to R4.20 or later.
The fix for vulnerability #4 is provided by that revision.
For vulnerability #1, #2, and #3, use the packet filter function in FCN and set to allow only communication from the appropriate source. Furthermore, take measures against the network so that communication data cannot be captured by untrusted third parties.

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.
https://contact.yokogawa.com/cs/gw?c-id=000498

ACKNOWLEDGMENTS:

Yokogawa sincerely thanks the following party.

- VDLab of Venustech

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

Revision History:

September 28, 2018	1st Edition

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