Yokogawa Security Advisory Report

YSAR-18-0006

Published on August 17, 2018
Last updated on August 17, 2018

YSAR-18-0006: Buffer overflow vulnerability in the license management function of YOKOGAWA products

Overview:

A buffer overflow vulnerability has been found in the license management function of YOKOGAWA products. 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.

- iDefine for ProSafe-RS (R1.16.3 or earlier)
- STARDOM (VDS R7.50 or earlier, FCN/FCJ Simulator R4.20 or earlier)
- ASTPLANNER (R15.01 or earlier)
- TriFellows (V5.04 or earlier)

Vulnerability:

If the license management function of a computer on which an affected product is installed receives specially crafted data, there is a risk that the license management function will be stopped or arbitrary programs will be executed.

CVSS v3 Base Score: 8.6, Temporal Score: 8.0

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:

By updating to the latest version or applying the patch, the vulnerability is corrected.

Affected Product	Latest version	Patch
iDefine for ProSafe-RS	R1.16.4	Planning to issue a patch
STARDOM	VDS R8.10	Issued a patch for VDS R7.50 and FCN/FCJ Simulator R4.20
ASTPLANNER	R15.02.01	Please contact the supports in the following section
TriFellows	V5.10	Please contact the supports in the following section

When Yokogawa service personnel perform system upgrade or install patches, those charges are borne by the customer.

Please contact the supports in the following section for the countermeasures regarding the affected products.

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.

- iDefine for ProSafe-RS, STARDOM
  https://contact.yokogawa.com/cs/gw?c-id=000498
- ASTPLANNER, TriFellows
  https://contact.yokogawa.com/cs/gw?c-id=000497

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.

2. ICS-CERT Vulnerability Note : VU#<vulnerability number>
   https://ics-cert.us-cert.gov/

Revision History:

August 17, 2018 1st Edition

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