Yokogawa Security Advisory Report

YSAR-19-0003

Published on Sep 27, 2019
Last updated on Sep 6, 2021

YSAR-19-0003: “Unquoted service path” vulnerability in Yokogawa Products Add quotes

Overview:

An “Unquoted service path vulnerability” has been found in Yokogawa products. 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:

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

- Exaopc (R3.01.00 - R3.77.00) *4
- Exaplog (R1.10.00 - R3.40.00)
- Exaquantum (R1.10.00 - R3.15.00) *1
- Exaquantum/Batch (R1.01.00 - R3.10.00) *2
- Exasmoc (All Revisions)
- Exarqe (All Revisions)
- GA10 (R1.01.01 - R3.05.01)
- InsightSuiteAE (R1.01.00 - R1.06.00)
- ProSafe-RS (R1.01.00 - R4.04.00)
- IA System Products Virtualization Platform (R1.01.00) *3
- PRM (R4.01.00 - R4.03.00)
- Field Wireless Device OPC Server (R2.01.00, R2.01.01, R2.01.03, R2.01.10)
- Exapilot (R1.01.00 - R3.98.10)
- STARDOM VDS (R4.01 - R8.10)
- STARDOM FCN/FCJ OPC Server for Windows (R1.01 - R4.20)

*1 Exaquantum R3.10.00 is affected by this vulnerability. (It was written as “Not Affected” in previous revision of this report.)
*2 Exaquantum/Batch R3.10.00 is affected by this vulnerability. (It was written as “Fixed revision” in previous revision of this report.)
*3 Only Thin Client is affected by this vulnerability.
*4 Model & Suffix Codes: Only NTPF100-SX is affected by this vulnerability.

Vulnerability:

The service path in some Yokogawa applications are unquoted and contain spaces.
When the service path is unquoted and contain spaces, a local attacker could execute malicious file by the service privilege.

CVSS v3 Base Score: 8.4, Temporal Score: 8.0
AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Countermeasures:

The countermeasure is different each product. Please check the following.

Products	Affected Revisions	Countermeasures
Exaopc (Only NTPF100-SX)	R3.01.00 - R3.77.00	Please consider the revision up to the latest revision (R3.78.00). This vulnerability has been fixed in R3.78.00.
Exaplog	R1.10.00 - R3.30.00	Please consider the revision up to the latest revision (R3.40.00) and applying patch software (R3.40.06).
	R3.40.00	Please apply patch software (R3.40.06).
Exaquantum	R1.10.00 - R3.10.00	Please consider the revision up to the latest revision (R3.20.00). This vulnerability has been fixed in R3.20.00.
	R3.15.00	Please apply patch software (R3.15.15) or consider the revision up to the latest revision (R3.20.00).
Exaquantum/Batch	R1.01.00 - R3.10.00	Please consider the revision up to the latest revision (R3.10.10). This vulnerability has been fixed in R3.10.10.
Exasmoc	All revisions	Exasmoc will be End-of-Support in Sep 30, 2019. Please consider the migration to Platform for Advanced Control and Estimation which is the successor to Exasmoc.
Exarqe	All revisions	Exarqe will be End-of-Support in Sep 30, 2019. Please consider the migration to Platform for Advanced Control and Estimation which is the successor to Exarqe.
GA10	R1.01.01 - R3.05.01	Please consider the revision up to the latest revision (R3.05.06). This vulnerability has been fixed in R3.05.02.
InsightSuiteAE	R1.01.00 - R1.06.00	Please consider the revision up to the latest revision (R1.07.00). This vulnerability has been fixed in R1.07.00.
ProSafe-RS	R1.01.00 - R4.04.00	Please consider the revision up to the latest revision (R4.05.00). This vulnerability has been fixed in R4.05.00.
IA System Products Virtualization Platform (Only Thin Client)	R1.01.00	Please consider the revision up to the latest revision (R1.01.10). This vulnerability has been fixed in R1.01.10.
PRM	R4.01.00 - R4.03.00	Please consider the revision up to the latest revision (R4.04.00). This vulnerability has been fixed in R4.04.00.
Field Wireless Device OPC Server	R2.01.00, R2.01.01, R2.01.03, R2.01.10	Please apply patch software R2.01.11.
Exapilot	R1.01.00 - R3.98.10	Please consider the revision up to the latest revision (R3.99.00). This vulnerability has been fixed in R3.99.00.
STARDOM VDS	R4.01 - R8.10	Please consider the revision up to the latest revision (R9.01.01). This vulnerability has been fixed in R9.01.01.
STARDOM FCN/FCJ OPC Server for Windows	R1.01 - R4.20	Please consider the revision up to the latest revision (R4.30.01). This vulnerability has been fixed in R4.30.01.

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

Yokogawa strongly suggest all customers to have 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 the security program and for 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.

Supports:

For questions related to this report, please contact the below.
https://contact.yokogawa.com/cs/gw?c-id=000498

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:

Sep 27, 2019	1st Edition
Oct 11, 2019	Updated “Affected Products” and “Countermeasures” (Exaquantum)
Oct 24, 2019	Updated “Countermeasures” (Exaquantum)
Nov 1, 2019	Updated “Countermeasures” (Exaquantum)
Jan 24, 2020	Added ProSafe-RS in “Affected Products” and “Countermeasures”
Jun 26, 2020	Added IA System Products Virtualization Platform and updated Exaquantum in “Affected Products” and “Countermeasures”
Jul 31, 2020	Updated Exaopc’s affected revision
Jul 5, 2021	Added PRM and Field Wireless Device OPC Server in “Affected Products” and “Countermeasures”
Sep 6, 2021	Added Exapilot and STARDOM VDS, STARDOM FCN/FCJ OPC Server for Windows in “Affected Products” and “Countermeasures”

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