Yokogawa Security Advisory Report

YSAR-19-0003

Published on Sep 27, 2019
Last updated on Nov 1, 2019

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 (R1.01.00 - R3.77.00)
- Exaplog (R1.10.00 - R3.40.00)
- Exaquantum (R1.10.00 - R3.02.00, R3.15.00)
- Exaquantum/Batch (R1.01.00 - R2.50.40)
- Exasmoc (All Revisions)
- Exarqe (All Revisions)
- GA10 (R1.01.01 - R3.05.01)
- InsightSuiteAE (R1.01.00 - R1.06.00)

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	R1.01.00 – 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 for R3.40.06.
	R3.40.00	Please apply patch software for R3.40.06.
Exaquantum	R1.10.00 - R3.02.00	Please consider the revision up to the latest revision

		(R3.15.00) and applying patch software for R3.15.15.
	R3.10.00	R3.10.00 is not affected by this vulnerability.
	R3.15.00	Please apply patch software for R3.15.15.
Exaquantum/Batch	R1.01.00 - R2.50.40	Please consider the revision up to the latest revision (R3.10.00). This vulnerability has been fixed in R3.10.00.
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.

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)

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