Yokogawa Security Advisory Report

YSAR-21-0001

Published on Apr 23, 2021
Last updated on Sep 6, 2021

YSAR-21-0001: Update of old version VB6 Runtime in Yokogawa products

Overview:

Yokogawa products in which old version VB6 runtime are installed have been found. 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:

- Exaopc R1.01.00 - R3.78.00
- Exaquantum R1.10.00 - R3.20.00
- ProSafe-RS R1.01.00 - R4.05.00 ※1
- CENTUM VP (Including Entry Class) R4.01.00 - R6.07.10 ※2
- PRM R2.01.00 - R4.03.00
- Field Wireless Device OPC Server R2.01.00, R2.01.01, R2.01.03, R2.01.10
- STARDOM VDS R4.01 - R8.10
- STARDOM FCN/FCJ OPC Server for Windows R1.01 - R4.20
- B/M9000 VP R7.01.01 - R8.03.00

※1 The following package affects.
RS4E5100 Safety System Engineering and Maintenance Function
RS4H2200 SOE OPC Interface Package

※2 The following package affects.
VP6P6930 SEM OPC Interface Package

Vulnerability:

Please refer to below URL regarding VB6 runtime vulnerabilities.
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-070?redirectedfrom=MSDN

Countermeasures:

This security update which is provided from Microsoft is for Visual Basic 6.0 Service Pack 6(VB6 SP6).
These Yokogawa products do not install VB6 SP6. So, the Yokogawa products cannot apply the security update. Please check the following countermeasures.

Products	Affected Revisions	Fixed revision	Countermeasures
Exaopc	R1.01.00 - R3.78.00	R3.78.10	Please update to R3.78.10 or later.
Exaquantum	R1.10.00 - R3.20.00	R3.20.02	Please update to R3.20.00 and applying patch software R3.20.02.
ProSafe-RS	R1.01.00 - R4.05.00	R4.06.00	Please update to R4.06.00 or later.
CENTUM VP	All revisions of R4 R6.01.00 - R6.07.10	R6.08.00	Please update to R6.08.00 or later.
	All revisions of R5	R5.04.D3	Please update to R5.04.20 and applying patch software R5.04.D3.
PRM	R2.01.00 - R4.03.00	R4.04.00	Please update to R4.04.00 or later.

Field Wireless Device OPC Server	R2.01.00, R2.01.01, R2.01.03, R2.01.10	R2.01.11	Please apply patch software R2.01.11.
STARDOM VDS	R4.01 - R8.10	R9.01	Please update to R9.01 or later.
STARDOM FCN/FCJ OPC Server for Windows	R1.01 - R4.20	R4.30.01	Please update to R4.30.01 or later.
B/M9000 VP	R7.01.01 - R8.03.01	R8.03.53	Please update to R8.03.01 and applying patch software R8.03.53.

When Yokogawa service personnel perform update, those charges are borne by the customer.

Yokogawa strongly recommends all customers to establish and maintain 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 and running the security program continuously. For considering the most effective risk mitigation plan, as 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

Revision History:

Apr 23, 2021: 1st Edition
Sep 6, 2021: Added STARDOM FCN/FCJ OPC Server for Windows in “Affected Products” and “Countermeasures”
* Contents of this report are subject to change without notice.