Yokogawa Security Advisory Report

YSAR-21-0004
Published on October 27, 2021
Last updated on October 27, 2021

YSAR-21-0004: Notification of the update of MSXML in Yokogawa products

Overview:

Yokogawa products in which old version of MSXML are installed have been found. The version is no longer supported by Microsoft. 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:

- Exaquantum R1.10.00 - R3.10.00
- Exaquantum/Batch R1.10.00 - R3.10.00
- ProSafe-RS R1.01.00 - R4.04.00
- CENTUM VP (Including Entry Class) R5.02.00 - R6.06.00
- PRM R2.01.00 - R4.02.00
- STARDOM VDS R4.01 - R8.10
- STARDOM FCN/FCJ R1.01 - R4.20
- WideField3 R1.01 - R4.04
- B/M9000 VP R7.02.01 - R8.02.04

Vulnerability:

The version of MSXML which is installed with the affected Yokogawa products is no longer supported by Microsoft. It is not provided bug fix and security update by Microsoft.

Countermeasures:

Products	Affected Revisions	Fixed revision	Countermeasures
Exaquantum	R1.10.00 - R3.10.00	R3.15.00	Please update to R3.15.00 or later.
Exaquantum/Batch	R1.10.00 - R3.10.00	R3.10.10	Please update to R3.10.00 and applying patch software R3.10.10. Or please update to R3.30.00 or later.
ProSafe-RS	R1.01.00 - R4.04.00	R4.05.00	Please update to R4.05.00 or later.
CENTUM VP	R5.02.00 - R6.06.00	R6.07.00	Please update to R6.07.00 or later.
PRM	R2.01.00 - R4.02.00	R4.03.00	Please update to R4.03.00 or later.
STARDOM VDS	R4.01 - R8.10	R9.01	Please update to R9.01 or later.
STARDOM FCN/FCJ	R1.01 - R4.20	R4.30.01	Please update to R4.30.01 or later.
WideField3	R1.01 - R4.04	R4.05	Please update to R4.05 or later.
B/M9000 VP	R7.02.01 - R8.02.04	-	This product is not affected by the vulnerabilities. However, this product is affected by the existence of CENTUM VP installed on the same PC. If installed CENTUM VP need to update, also please update B/M9000 VP to suitable revision.

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.
(Except for WideField3)
https://contact.yokogawa.com/cs/gw?c-id=000498

For questions related to WideField3, please contact the below.
https://www.yokogawa.com/solutions/products-platforms/control-system/programmable-logic-controllers-plc-pac/
> Contact Us

Revision History:

October 27, 2021: 1st Edition
* Contents of this report are subject to change without notice.