Yokogawa Security Advisory Report

YSAR-23-0002
Published on October 20, 2023
Last updated on October 20, 2023

YSAR-23-0002: Affected Yokogawa products by Expat (libexpat) vulnerabilities

Overview:

Yokogawa products that are affected by vulnerabilities in the XML parser library "Expat (libexpat)“ has 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:

This vulnerability affects the following products.

- Network Switch for Vnet/IP

Type	Revision
GRVSW-663FA, GRVSW-664FA, GRVSW-665FA, GRVSW-666FA, GRVSW-667FA, GRVSW-668FA, GRVSW-669FA, GRVSW-670FA, GRVSW-671FA, GRVSW-672FA, GRVSW-673FA, GRVSW-660FA, GRVSW-661FA, GRVSW-662FA	Software Release 09.1.07 or earlier

Vulnerability:

For more information about the Expat (libexpat) vulnerability, please refer to the following site.

CVE-2022-40674, CVE-2022-43680
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40674
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-43680

Countermeasures:

- Network Switch for Vnet/IP

Type	Revision	Countermeasures
GRVSW-663FA, GRVSW-664FA, GRVSW-665FA, GRVSW-666FA, GRVSW-667FA, GRVSW-668FA, GRVSW-669FA, GRVSW-670FA, GRVSW-671FA, GRVSW-672FA, GRVSW-673FA, GRVSW-660FA, GRVSW-661FA, GRVSW-662FA	Software Release 09.1.07 or earlier	Please revision up to the 09.1.08 or later (*)

* If the customer wishes to revision up, please ask our sales or service staff.

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.

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:

October 20, 2023:	1st Edition

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