Yokogawa Security Advisory Report

YSAR-14-0004E
Published on November 28, 2014
Last updated on December 22, 2017

YSAR-14-0004E: XML External Entity (XXE) processing Vulnerability in FAST/TOOLS

Overview:

SCADA software FAST/TOOLS has been found with a XML external entity processing vulnerability. After the investigation, Yokogawa identified the range of products that could be influenced by the vulnerability and summarized the countermeasures in this document.

Go over the report and confirm which products are affected in order to consider security measures for the overall systems. Also please consider applying the countermeasures introduced here as needed.

Affected Products:

Following are the products that would be affected by the vulnerability reported in this document.
Any computer on which these products are installed has vulnerability.

FAST/TOOLS (R9.01～R9.05)

Vulnerability

<Condition of occurrence: An attacker intrudes into the WebHMI server in any way>

In case an attacker edits specific file on the WebHMI server, the following events could occur:

- Information in the WebHMI server could be sent to an outside machine
- Potential to increase the load of the WebHMI server and the network which could adversely affect the performance of SCADA functionality.

The occurrence of the event, an attacker must intrude into the WebHMI server in any way. Therefore, if the WebHMI server is kept secure, possibility of the occurrence of the event is very low.

CVSS Base Score: 2.4, Temporal Score: 2.0

Access Vector:	Local
Access Complexity:	High
Authentication:	Single
Confidentiality Impact (C):	Partial
Integrity Impact (I):	None
Availability Impact (A):	Partial
Exploitability:	Functional
Remediation Level:	Official Fix
Report Confidence:	Confirmed

Countermeasures:

If the intrusion risk to the WebHMI server by the attacker is unacceptable level, or the risk is acceptable level but you want to reduce the risk of the occurrence of the event, please fix this vulnerability.

By installing the service pack (R9.05-SP2) for the FAST/TOOLS R9.05, the vulnerability found this time is corrected.

- To activate the service pack, the computer needs to be rebooted.
- In case the system uses earlier revision (R9.01 – R9.04) than the target revision (R9.05), please upgrade to the target revision (R9.05) and then apply for the service pack. Contact Yokogawa supports & services when your system is difficult to update to the target revision (R9.05).

In addition, the vulnerability will be corrected also be upgrade to the latest version (R10.01) of FAST/TOOLS.

When Yokogawa service personnel perform the above practical tasks, those charges are borne by the customer.

Yokogawa strongly suggests all customers to introduce appropriate security measures not only for the vulnerability identified but also to the overall systems.

Acknowledgement:

Yokogawa thanks to the following organizations and persons for their support and cooperation in finding the FAST/TOOLS vulnerability.

- Timur Yunusov, Alexey Osipov , and Ilya Karpov of Positive Technologies Inc.
- JPCERT/CC

Supports and Services:

For questions related to this document or how to obtain the patch software, please contact Yokogawa service department or access the below URL for more details.
https://contact.yokogawa.com/cs/gw?c-id=000037

Reference:

1. A Complete Guide to the Common Vulnerability Scoring System (CVSS)
   http://www.first.org/cvss/cvss-guide.pdf
   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 has to be judged by the users considering the security measures equipped with the overall systems.

Revision History:

November 28, 2014 1st Edition
December 22, 2017 2nd Edition: URL in Supports and Services is updated.

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