Yokogawa Security Advisory Report

YSAR-24-0001

Published on June 26, 2024
Last updated on July 4, 2024

YSAR-24-0001: Vulnerabilities in FAST/TOOLS and CI Server

Overview:

Vulnerabilities has been found in FAST/TOOLS and CI Server. Yokogawa has identified the range of affected products in this report.
Please 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.

Product name	Affected Versions	Affected Package
FAST/TOOLS	R9.01 - R10.04	RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB
Collaborative Information Server (CI Server)	R1.01.00 – R1.03.00	All package

Vulnerability 1:

The affected product's WEB HMI server's function to process HTTP requests has a security flaw (Reflected XSS) that allows the execution of malicious scripts.
Therefore, if a client PC with inadequate security measures accesses a product URL containing a malicious request, the malicious script may be executed on the client PC.

CWE-79 : Cross-site Scripting
CVE: CVE-2024-4105
CVSS v3 Base score: 5.8
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Vulnerability 2:

The affected products have built-in accounts with no passwords set.
Therefore, if the product is operated without a password set by default, an attacker can break into the affected product.

CWE-258 : Empty Password in Configuration File
CVE: CVE-2024-4106
CVSS v3 Base score: 5.3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Countermeasures:

Product name	Affected Revisions	Fixed Revision	Countermeasures
FAST/TOOLS	R9.01 - R10.04	I12560 *1	Please revision up to the R10.04 and apply patch software (I12560) after apply patch software (R10.04 SP3). Also, if the password for the default account has not been changed, please change that password according to the documentation included with the patch software.
Collaborative Information Server (CI Server)	R1.01.00 – R1.03.00	R1.03.0F *1	Please revision up to the R1.03.00 and apply patch software (R1.03.0F). Also, if the password for the default account has not been changed, please change that password according to the documentation included with the patch software.

*1: This patch software provides security enhancements in addition to the vulnerabilities reported in this document.

Yokogawa recommends updating as above the countermeasures. 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.

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 has to be judged by the users considering the security measures equipped with the overall systems.

Revision History:

June 26, 2024:	1st Edition	
June 26, 2024:	2nd Edition	Correction of CVSS in Vulnerability 2
July 4, 2024:	3rd Edition	Added note of caution

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