Yokogawa Security Advisory Report

YSAR-26-0004

Published on June 23, 2026
Last updated on June 23, 2026

YSAR-26-0004: FAST/TOOLS and CI Server vulnerable to cleartext transmission of sensitive information

Overview:
A vulnerability 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:
These vulnerabilities affect the following product.

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

Vulnerability:
The web server may return a response containing the CI Server setting information. This information could be exploited by an attacker for other attacks.

CWE-319: Cleartext Transmission of Sensitive Information
CVE: CVE-2026-11833
CVSS v3 Base score: 7.5
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v4 Base score: 8.2
CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Countermeasures:

Product name	Affected Revisions	Fixed Revision	Countermeasures
FAST/TOOLS	R9.01 - R10.04	R10.04 SP4	Please revision up to the R10.04 and apply patch software (R10.04 SP4).
Collaborative Information Server (CI Server)	R1.01 – R1.04	R1.04	Please revision up to the R1.05.

 # Regarding the vulnerabilities described in this report
The vulnerabilities described in this report do not constitute non-conformities of the affected products. Therefore, if a customer requests Yokogawa to perform work related to the countermeasures described in this report, the associated costs will be borne by the customer.

 # Recommendation for countermeasures
To help reduce cybersecurity risks, Yokogawa recommends applying the countermeasures described in this

report.
However, the actual impact of the vulnerabilities described in this report may vary depending on each customer's system environment. We recommend that customers carefully review this report and determine whether and when to apply the countermeasures based on a risk assessment of their system environment.

Yokogawa offers support for applying the countermeasures described in this report, as well as assistance with other cybersecurity measures. Please contact your local Yokogawa supporting office for further information or support.

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 23, 2026: 1st Edition

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