Yokogawa Security Advisory Report

YSAR-26-0001

Published on February 9, 2026
Last updated on February 9, 2026

YSAR-26-0001: Vulnerabilities in FAST/TOOLS

Overview:

Vulnerabilities have been found in FAST/TOOLS. 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

Vulnerability 1:

Detailed messages are displayed on the error page. This information could be exploited by an attacker for other attacks.

CWE-209: Generation of Error Message Containing Sensitive Information
CVE: CVE-2025-66594
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
CVSS v4 Base score: 6.9
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Vulnerability 2:

This product is vulnerable to Cross-Site Request Forgery (CSRF). When a user accesses a link crafted by an attacker, the user's account could be compromised.

CWE-352: Cross-Site Request Forgery (CSRF)
CVE: CVE-2025-66595
CVSS v3 Base score: 5.3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v4 Base score: 6.3
CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Vulnerability 3:

This product does not properly validate request headers. When an attacker inserts an invalid host header, users could be redirected to malicious sites.

CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
CVE: CVE-2025-66596
CVSS v3 Base score: 5.8
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N
CVSS v4 Base score: 6.9
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N

Vulnerability 4:
This product supports weak cryptographic algorithms, potentially allowing an attacker to decrypt communications with the web server.

CWE-327: Use of a Broken or Risky Cryptographic Algorithm
CVE: CVE-2025-66597
CVSS v3 Base score: 8.2
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v4 Base score: 8.8
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

Vulnerability 5:
This product supports old SSL/TLS versions, potentially allowing an attacker to decrypt communications with the web server.

CWE-327: Use of a Broken or Risky Cryptographic Algorithm
CVE: CVE-2025-66598
CVSS v3 Base score: 7.1
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
CVSS v4 Base score: 7.1
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

Vulnerability 6:
Physical paths could be displayed on web pages. This information could be exploited by an attacker for other attacks.

CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere
CVE: CVE-2025-66599
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
CVSS v4 Base score: 6.9
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Vulnerability 7:
This product lacks HSTS (HTTP Strict Transport Security) configuration. When an attacker performs a Man in the middle (MITM) attack, communications with the web server could be sniffed.

CWE-358: Improperly Implemented Security Check for Standard
CVE: CVE-2025-66600
CVSS v3 Base score: 8.2
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v4 Base score: 8.8
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

Vulnerability 8:
This product does not specify MIME types. When an attacker performs a content sniffing attack, malicious scripts could be executed.

CWE-358: Improperly Implemented Security Check for Standard
CVE: CVE-2025-66601
CVSS v3 Base score: 6.5
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v4 Base score: 6.3
CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Vulnerability 9:
The web server accepts access by IP address. When a worm that randomly searches for IP addresses intrudes into the network, it could potentially be attacked by the worm.

CWE-291: Reliance on IP Address for Authentication
CVE: CVE-2025-66602
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
CVSS v4 Base score: 6.9
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Vulnerability 10:
The web server accepts the OPTIONS method. An attacker could potentially use this information to carry out other attacks.

CWE-358: Improperly Implemented Security Check for Standard
CVE: CVE-2025-66603
CVSS v3 Base score: 3.1
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS v4 Base score: 2.1
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Vulnerability 11:
The library version could be displayed on the web page. This information could be exploited by an attacker for other attacks.

CWE-319: Cleartext Transmission of Sensitive Information
CVE: CVE-2025-66604
CVSS v3 Base score: 3.1
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS v4 Base score: 2.1
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Vulnerability 12:
Since there are input fields on this webpage with the autocomplete attribute enabled, the input content could be saved in the browser the user is using.

CWE-359: Exposure of Private Personal Information to an Unauthorized Actor
CVE: CVE-2025-66605
CVSS v3 Base score: 3.1
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS v4 Base score: 2.1
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Vulnerability 13:
This product does not properly encode URLs. An attacker could tamper with web pages or execute malicious scripts.

CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages
CVE: CVE-2025-66606
CVSS v3 Base score: 3.4
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N
CVSS v4 Base score: 2.1
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N

Vulnerability 14:
The response header contains an insecure setting. Users could be redirected to malicious sites by an attacker.

CWE-358: Improperly Implemented Security Check for Standard
CVE: CVE-2025-66607
CVSS v3 Base score: 3.7
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v4 Base score: 6.3

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Vulnerability 15:
This product does not properly validate URLs. An attacker could send specially crafted requests to steal files from the web server.

CWE-29: Path Traversal
CVE: CVE-2025-66608
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: 8.7
CVSS:4.0/AV:N/AC:L/AT:N/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	CS_e12787	Please revision up to the R10.04 and apply patch software (CS_e12787) after apply patch software (R10.04 SP3).

 # 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:
February 9, 2026: 1st Edition

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