Yokogawa Security Advisory Report

YSAR-26-0004

公開日 2026-6-23
最終更新日 2026-6-23

YSAR-26-0004: FAST/TOOLS と CI Server における重要情報の平文送信の脆弱性

概要:
FAST/TOOLS と CI Server に重要情報の平文送信の脆弱性が存在することを確認しました。以下に、影響を受ける製品をご案内いたします。
本レポートの内容をご確認の上、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的にご判断いただき、必要に応じて対策の適用をご検討ください。

影響を受ける製品:
下記製品に脆弱性が存在します。

製品名	影響を受けるパッケージ	影響を受けるバージョン
FAST/TOOLS	RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB	R9.01 - R10.04
統合情報サーバ（CI サーバ）	全てのパッケージ	R1.01 - R1.04

脆弱性詳細:
Web サーバが設定情報を含む応答を返す可能性があります。攻撃者はその情報を利用することにより、他の攻撃を行う可能性があります。

CWE-319: 重要な情報の平文での送信
CVE: CVE-2026-11833
CVSS v3 基本値: 7.5
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v4 基本値: 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

対策方法:

製品名	影響を受けるバージョン	修正バージョン	対策方法
FAST/TOOLS	R9.01 - R10.04	R10.04 SP4	R10.04 へレビジョンアップの上、パッチ版 (R10.04 SP4) を適用してください。
統合情報サーバ（CI サーバ）	R1.01 - R1.04	R1.05	R1.05 へレビジョンアップしてください。

 # 本レポートで説明された脆弱性について
本レポートで説明された脆弱性は影響を受ける製品の不適合ではありません。
そのため、本レポートで説明された対策に関する作業を横河にご依頼いただいた場合、当該作業にかかる費用はお客様負担となります。

 # 対策についての推奨事項
サイバーセキュリティリスクの低減のために、横河は本レポートで説明された対策の適用を推奨します。

なお本レポートで報告されている脆弱性の実際の影響度は、各お客様固有のシステム環境によって異なります。お客様が本レポートを参考に、本レポートで説明された対策を適用するかどうか、いつ適用するか等について判断される事を推奨します。

横河では本レポートで説明された対策の適用に関するご相談、および各種セキュリティ対策についてのご相談も承っています。詳細な情報または支援が必要な場合は、弊社サービス拠点までお問い合わせください。

サポート:

本レポートの内容に関するご質問等については、下記サイトからお問い合わせください。
https://contact.yokogawa.com/cs/gw?c-id=000523

参考:

1. CVSS（共通脆弱性評価システム）について
   https://www.first.org/cvss/
   共通脆弱性評価システム CVSS （Common Vulnerability Scoring System）は、情報システムの脆弱性に対するベンダーに依存しない汎用的な評価手法です。脆弱性の深刻度を同一の基準の下で定量的に比較できるようになります。
   本レポートに記載されている CVSS の各値は現状のまま提供するものであり、いかなる保証も伴いません。
   本レポートに記載されている脆弱性が実際にどれだけの深刻度があるかについては、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的に判断した上で、お客様自身で評価していただく必要があります。

更新履歴:

2026-6-23: 初版

※本レポートの内容については、将来予告なしに変更することがあります。