Yokogawa Security Advisory Report

YSAR-26-0001

公開日 2026-2-9
最終更新日 2026-2-9

YSAR-26-0001: FAST/TOOLS に複数の脆弱性

概要:
FAST/TOOLS に複数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

脆弱性詳細 1:
エラーページに詳細なメッセージが表示されます。この情報は、攻撃者により他の攻撃に悪用される可能性があります。

CWE-209: エラーメッセージによる情報漏えい
CVE: CVE-2025-66594
CVSS v3 基本値: 5.3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS v4 基本値: 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

脆弱性詳細 2:
クロスサイトリクエストフォージェリ(CSRF)に対して脆弱であるため、攻撃者により細工されたリンクへアクセスした場合、アカウントが成りすまされる可能性があります。

CWE-352: クロスサイトリクエストフォージェリ
CVE: CVE-2025-66595
CVSS v3 基本値: 5.3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v4 基本値: 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

脆弱性詳細 3:
リクエストヘッダーの検証が不十分であるため、攻撃者が無効なホストヘッダーを挿入した場合、不正なホストへリダイレクトされる可能性があります。

CWE-601: オープンリダイレクト
CVE: CVE-2025-66596

CVSS v3 基本値: 5.8
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N
CVSS v4 基本値: 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

脆弱性詳細 4:
弱い暗号アルゴリズムが使用可能であるため、攻撃者により Web サーバーとの通信を解読される可能性があります。

CWE-327: 不完全、または危険な暗号アルゴリズムの使用
CVE: CVE-2025-66597
CVSS v3 基本値: 8.2
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v4 基本値: 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

脆弱性詳細 5:
古い SSL/TLS バージョンが使用可能であるため、攻撃者により Web サーバーとの通信を解読される可能性があります。

CWE-327: 不完全、または危険な暗号アルゴリズムの使用
CVE: CVE-2025-66598
CVSS v3 基本値: 7.1
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
CVSS v4 基本値: 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

脆弱性詳細 6:
Web ページに物理パスが表示される可能性があります。この情報は、攻撃者により他の攻撃に悪用される可能性があります。

CWE-497: 認可されていない制御領域への重要情報の漏洩
CVE: CVE-2025-66599
CVSS v3 基本値: 5.3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS v4 基本値: 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

脆弱性詳細 7:
HSTS(HTTP Strict Transport Security)が設定されていません。攻撃者により中間者攻撃(Man-in-the-Middle Attack)が行われた場合、Web サーバーとの通信内容を窃取される可能性があります。

CWE-358: 不適切に実装されたセキュリティチェック
CVE: CVE-2025-66600
CVSS v3 基本値: 8.2
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v4 基本値: 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

脆弱性詳細 8:
MIME タイプを指定していないため、攻撃者により Content Sniffing 攻撃が行われた場合、不正なスクリプトを実行される可能性があります。

CWE-358: 不適切に実装されたセキュリティチェック
CVE: CVE-2025-66601
CVSS v3 基本値: 6.5
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v4 基本値: 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

脆弱性詳細 9:
Web サーバーが IP アドレスによるアクセスを受け付けるため、ランダムな IP アドレスで Web サーバーを探すワームがネットワーク内へ侵入した場合、攻撃される可能性があります。

CWE-291: 認証時の IP アドレスへの依存
CVE: CVE-2025-66602
CVSS v3 基本値: 5.3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS v4 基本値: 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

脆弱性詳細 10:
Web サーバーは OPTIONS メソッドを受け付けます。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-358: 不適切に実装されたセキュリティチェック
CVE: CVE-2025-66603
CVSS v3 基本値: 3.1
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS v4 基本値: 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

脆弱性詳細 11:
Web ページにライブラリのバージョンが表示される可能性があります。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-2025-66604
CVSS v3 基本値: 3.1
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS v4 基本値: 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

脆弱性詳細 12:
Web ページに Autocomplete 属性を有効にしている入力項目があるため、ブラウザに入力内容が保存される可能性があります。

CWE-359: 認可されていない行為者への個人情報の漏洩
CVE: CVE-2025-66605
CVSS v3 基本値: 3.1
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS v4 基本値: 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

脆弱性詳細 13:
URL のエンコード処理が不十分であるため、Web ページの改ざんや不正なスクリプトを実行される可能性が

あります。

CWE-86: Web ページ内の識別子における無効な文字の不適切な無害化
CVE: CVE-2025-66606
CVSS v3 基本値: 3.4
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N
CVSS v4 基本値: 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

脆弱性詳細 14:
レスポンスヘッダーにセキュアでない設定があります。攻撃者により不正なサイトへ誘導される可能性があります。

CWE-358: 不適切に実装されたセキュリティチェック
CVE: CVE-2025-66607
CVSS v3 基本値: 3.7
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v4 基本値: 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

脆弱性詳細 15:
URL の検証が不十分であるため、攻撃者により細工されたリクエストを送信され、Web サーバー内のファイルを窃取される可能性があります。

CWE-29: パストラバーサル
CVE: CVE-2025-66608
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: 8.7
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

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	CS_e12787	R10.04 へレビジョンアップの上、パッチ版(R10.04 SP3)を適用後に、パッチ版(CS_e12787)を適用してください。

 # 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:
2026-2-9: 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。