Yokogawa Security Advisory Report

YSAR-26-0003

公開日 2026-03-27
最終更新日 2026-03-27

YSAR-26-0003: CENTUM にハードコードパスワードの脆弱性

概要:
CENTUM にハードコードパスワード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。
・CENTUM シリーズ

	影響を受けるレビジョン	影響を受ける機能
CENTUM VP (CENTUM VP Basic 含む)	R5.01.00 - R5.04.20	LHS1100/LHM1101 操作監視基本機能 (CENTUM 認証モードの場合、影響あり)
	R6.01.00 - R6.12.00	VP6H1100 操作監視基本機能 (CENTUM 認証モードの場合、影響あり)
	R7.01.00	VP7H1100 操作監視基本機能 (CENTUM 認証モードの場合、影響あり)

脆弱性詳細:
影響を受ける製品にはシステムで使用する CENTUM 認証用のユーザー(PROG)のハードコードされたパスワードが存在します。下記の状況下において攻撃者に PROG ユーザーでユーザーインされるリスクがあります。
PROG ユーザーのデフォルト権限は S1 権限（OFFUSER 相当）なので、適切に権限設定された操作監視対象の場合は、ユーザーインされたとしても重要な操作や設定変更をされるリスクは低いと考えられます。
（何らかの理由で PROG ユーザーの権限を変更してしまっている場合は、変更した権限での操作や設定変更をされるリスクがあります。下記 CVSS 値はデフォルト権限のままだった場合の値です。）
また、本脆弱性を利用するには攻撃者が HIS の画面操作ができる状況になっている必要があるため、その時点で本脆弱性と関係なく攻撃者が操作監視可能になってしまっています。

脆弱性の影響を受ける状況：
下記の全ての条件を満たしている場合、脆弱性の影響を受ける状況となります。
・攻撃者が何らかの方法でハードコードされたパスワードを入手する
・影響を受ける製品がインストールされた HIS が CEMTUM 認証モードになっている
・攻撃者が直接上記 HIS にアクセスできる、またはリモートから何らかの方法で上記 HIS に侵入し、画面操作ができる

CWE-259 ： ハードコードされたパスワードの使用
CVE: CVE-2025-7741
CVSS v3 基本値:4.0
CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v4 基本値: 2.1
CVSS:4.0/AV:L/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

対策方法:

	影響を受けるレビジョン	修正 Rev	対策方法
CENTUM VP (CENTUM VP Basic 含む)	R5.01.00 - R5.04.20	なし	ユーザー認証モードを Windows 認証モードに変更してください。（※）
	R6.01.00 - R6.12.00		
	R7.01.00	R7.01.10	パッチ版(R7.01.10)を適用してください。

※Windows 認証モードへの変更にはエンジニアリング作業が必要となります。
変更を希望する場合は、弊社営業またはサービス担当に依頼してください。
変更作業のコストはお客様負担となります。

 # 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.ipa.go.jp/security/vuln/CVSSv3.html
   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:
2026-03-27: 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。