

# Yokogawa Security Advisory Report

YSAR-22-0006

公開日 2022-05-27  
最終更新日 2022-07-27

## YSAR-22-0006: CAMS for HIS にデータ漏洩／改ざん、リソース枯渇の脆弱性

### 概要:

CENTUM で動作するに CAMS for HIS にデータ漏洩／改ざん、リソース枯渇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

CENTUM CS 3000 (CENTUM CS 3000 Small 含む)	R3. 08. 10 - R3. 09. 00	LHS4800 (CAMS for HIS) をインストールしている場合に脆弱性の影響を受けます
CENTUM VP (CENTUM VP Small, CENTUM VP Basic 含む)	R4. 01. 00 - R4. 03. 00	CAMS 機能を使用している場合、脆弱性の影響を受けます
	R5. 01. 00 - R5. 04. 20	CAMS 機能を使用している/していないに関わらず脆弱性の影響を受けます
	R6. 01. 00 - R6. 09. 00	

- ・ Exaopc (R3. 72. 00 - R3. 80. 00) (NTPF100-S6「CENTUM VP 用 CAMS for HIS 対応」をインストールしている場合に脆弱性の影響を受けます)
- ・ B/M9000CS (R5. 04. 01 - R5. 05. 01)
- ・ B/M9000 VP (R6. 01. 01 - R8. 03. 01)

### 脆弱性詳細:

攻撃者が何らかの方法で同製品がインストールされたコンピューターに侵入できた場合、当該コンピューターに格納されているアカウント、パスワードを用いて、別の CAMS for HIS が管理するデータが漏洩／改ざんされる可能性があります。また、同アカウント、パスワードを用いて、別の CAMS for HIS に不要なファイルを作成するリソース枯渇攻撃がおこなわれ、最終的に CAMS for HIS の機能を停止させられる可能性があります。

- ・セキュリティ設計の原則に反した設計 ([CWE-657](#))
- CVE: [CVE-2022-30707](#)  
CVSS v3 基本値: 6.4  
[CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H](#)

**対策方法:**

	影響を受ける レビジョン	修正 Rev	対策方法
CENTUM CS 3000 CENTUM CS 3000 Small	R3.08.10 - R3.09.00	-	保守フェーズ期間終了製品の為、対策(パッチ版)は提供されません。 最新の CENTUM VP へのマイグレーションをご検討ください。
CENTUM VP CENTUM VP Small CENTUM VP Basic	R4.01.00 - R4.03.00		
	R5.01.00 - R5.04.20		
	R6.01.00 - R6.09.00	R6.09.03	R6.09.00 へレビジョンアップの上、パッチ版 (R6.09.03) を適用してください。
Exaopc	R3.72.00 - R3.80.00	R3.80.01	R3.80.00 へレビジョンアップの上、パッチ版 (R3.80.01) を適用してください。
B/M9000CS	R5.04.01 - R5.05.01	-	同製品自体には脆弱性の影響はありません。 一緒にインストールされる CENTUM が脆弱性の影響を受けるため、そちらをご確認ください。 最新の CENTUM VP にレビジョンアップする場合は、B/M9000 VP も適切なレビジョンにレビジョンアップしてください。
B/M9000 VP	R6.01.01 - R8.03.01		

横河は上記の対策方法に記載されている通り、アップデートを推奨します。

アップデート作業を横河電機にご依頼いただいた場合、同作業のコストはお客様負担となります。

今回確認された脆弱性に限らず、システム全体において適切なセキュリティ対策を講じていただくことを横河は推奨しています。対策例としては、パッチ適用、アンチウィルス、ホワイトリスティング、ハードニング、バックアップ、ファイアウォール、ネットワークセグメンテーション、などがあります。

**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>

**謝辞:**

本脆弱性は以下の方々により発見・通知されました。

- Jacob Baines from Dragos, Inc

**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>

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:**

2022-05-27: 初版

2022-07-27: 第 2 版: CVE を追加

※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。