Yokogawa Security Advisory Report

YSAR-22-0008

公開日 2022-07-29
最終更新日 2022-07-29

YSAR-22-0008: CENTUM コントローラーFCS にサービス運用妨害(DoS)の脆弱性

概要:
CENTUM コントローラーFCS にサービス運用妨害(DoS)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:
・CENTUM VP / CS 3000 コントローラー FCS
  ・CP31, CP33, CP345
  ・CP401, CP451

対象となるレビジョンの詳細については下記の対策方法をご確認ください。

脆弱性詳細:
CENTUM VP / CS 3000 コントローラー FCS が不正なパケットによる DoS 攻撃を受けた場合、ADL 通信が停止する可能性があります。

・リソース管理の問題(CWE-399)
CVE: CVE-2022-33939
CVSS v3 基本値: 6.5
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

対策方法:
CENTUM VP / CS 3000 コントローラー FCS
・CP31, CP33, CP345

	影響を受けるレビジョン	対策方法
CENTUM CS 3000 CENTUM CS 3000 Small	全てのレビジョン	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。

・CP401, CP451

	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	全てのレビジョン	-	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	R5.04.78	R5.04.20 へレビジョンアップの上、パッチ版（R5.04.78）を適用してください。
	R6.01.00 - R6.03.00	R6.03.10	R6.03.10 以上へレビジョンアップしてください。

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

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:
2022-07-29: 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。