Yokogawa Security Advisory Report

YSAR-18-0001

公開日 2018-01-22
最終更新日 2018-01-22

YSAR-18-0001: CENTUM と Exaopc にアラームの偽造と妨害の脆弱性

概要:

CENTUM または Exaopc がインストールされたコンピュータで、メッセージ管理機能にアラームの偽造と妨害の脆弱性が存在することを確認しました。以下に、この脆弱性の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:

下記影響を受ける製品がインストールされたコンピュータに脆弱性が存在します。

・CENTUM シリーズ
　CENTUM CS 1000　（全レビジョン）
　CENTUM CS 3000　（R3.09.50 およびそれ以前）
　CENTUM CS 3000 Small　（R3.09.50 およびそれ以前）
　CENTUM VP　（R6.03.10 およびそれ以前）
　CENTUM VP Small　（R6.03.10 およびそれ以前）
　CENTUM VP Basic　（R6.03.10 およびそれ以前）
・Exaopc　（R3.75.00 およびそれ以前）
・B/M9000CS　（全レビジョン）
・B/M9000 VP　（R8.01.01 およびそれ以前）

脆弱性概要

影響を受ける製品がインストールされたコンピュータに攻撃者が何らかの方法で侵入できた場合、メッセージ管理機能の脆弱性を利用して、下記の攻撃を実行されるリスクがあります。
・偽造アラームの発報
　製品のメッセージ管理サービスに対して、偽のシステムアラームやプロセスアラームを発報することができます。
・アラーム通知の妨害
　本来画面に表示されるはずだったシステムアラームやプロセスアラームを表示できなくさせることができます。

CVSS v2 における本脆弱性の基本値は 5.9、現状値は 4.6 です。

攻撃元区分(AV)	ローカル(L)	隣接(A)		ネットワーク(N)
攻撃条件の複雑さ(AC)	高(H)	中(M)		低(L)
攻撃前の認証要否(Au)	複数(M)	単一(S)		不要(N)
機密性への影響(C)	なし(N)	部分的(P)		全面的(C)
完全性への影響(I)	なし(N)	部分的(P)		全面的(C)
可用性への影響(A)	なし(N)	部分的(P)		全面的(C)

攻撃される可能性(E)	未実証(U)	実証可能(POC)	攻撃可能(F)	容易に攻撃可能(H)	未評価(ND)
利用可能な対策レベル(RL)	正式(OF)	暫定(TF)	非公式(W)	なし(U)	未評価(ND)
脆弱性情報の信頼性(RC)	未確認(UC)	未確証(UR)	確認済(C)	未評価(ND)	

対策方法:

下記パッチ版を適用または最新レビジョンにレビジョンアップすることで今回確認された脆弱性が修正されます。

製品名	影響を受けるレビジョン	対策方法
CENTUM CS 1000	全レビジョン	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 CS 3000 CENTUM CS 3000 Small	R3.09.50 およびそれ以前	
CENTUM VP CENTUM VP Small CENTUM VP Basic	R4.03.00 およびそれ以前	
	R5.04.20 およびそれ以前	R5.04.20 用パッチ版(R5.04.B2)
	R6.03.10 およびそれ以前	R6.04.00 で修正済み
Exaopc	R3.75.00 およびそれ以前	R3.76.00 で修正済み
B/M9000CS	全レビジョン	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ている CENTUM CS 3000 もしくは CS 1000 が脆弱性の影響を受けるのでご確認ください。
B/M9000 VP	R8.01.01 およびそれ以前	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ている CENTUM VP が脆弱性の影響を受けるのでご確認ください。 CENTUM VP をレブアップする場合は、B/M9000 VP も適切なレビジョンにレブアップしてください。

レビジョンアップ作業またはパッチ版適用作業について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。

直ちに本対策の適用が難しい場合は、当面、下記軽減策を実施頂く事により、今回確認された脆弱性のリスクを軽減する事が可能です。

なお、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推奨いたします。

軽減策:

ネットワーク経由で直接本脆弱性を利用した攻撃はできません。そのため影響を受ける製品がインストールされたコンピュータにおいて下記のようなマルウェア対策(セキュリティ対策)を施し、攻撃者に侵入されないようにする事で、本脆弱性が悪用されるリスクを軽減できます。

- ・アンチウイルスソフトウェアの導入
- ・ホワイトリスティングソフトウェアの導入
- ・USB メモリなどのリムーバブルメディアを経由するマルウェアの侵入経路対策の導入

これらのマルウェア対策として、弊社のエンドポイントセキュリティ対策サービスをご利用ください。

サポート:

本ドキュメントの内容に関するご質問については、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
   http://www.ipa.go.jp/security/vuln/CVSS.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。
   本ドキュメン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。本ドキュメン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、お客様ご自身で評価していただく必要があります。

更新履歴:

2018-01-22: 初版

※本ドキュメン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。

以上