Yokogawa Security Advisory Report

YSAR-15-0003

公開日 2015-09-10
最終更新日 2017-12-22

YSAR-15-0003: CENTUM を含む YOKOGAWA 製品の通信機能に複数の脆弱性

概要:

CENTUM を含む YOKOGAWA 製品がインストールされたコンピュータで、通信機能に複数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と、対策方法をご案内いたします。 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。

セキュリティ対策はお客様の重要な課題の 1 つであると、弊社は位置付けています。YOKOGAWA は継続的にソフトウェアのセキュリティ強化を行っており、早い段階で最新版のソフトウェアへのアップグレードをお勧めいたします。

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 (R3.08.70 およびそれ以前)
　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 (R6.02.00 およびそれ以前)
　CENTUM VP Small (R6.02.00 およびそれ以前)
　CENTUM VP Basic (R6.02.00 およびそれ以前)
・ProSafe-RS (R3.02.20 およびそれ以前)
・Exaopc (R3.73.00 およびそれ以前)
・Exaquantum (R2.85.00 およびそれ以前)
・Exaquantum/Batch (R2.50.30 およびそれ以前)
・Exapilot (R3.96.10 およびそれ以前)
・Exaplog (R3.40.00 およびそれ以前)
・Exasmoc (R4.03.20 およびそれ以前)
・Exarqe (R4.03.20 およびそれ以前)
・フィールド無線用 OPC サーバ (R2.01.02 およびそれ以前)
・PRM (R3.12.00 およびそれ以前)
・STARDOM VDS (R7.30.01 およびそれ以前)
・STARDOM OPC Server for Windows (R3.40 およびそれ以前)
・FAST/TOOLS (R10.01 およびそれ以前)
・B/M9000CS (R5.05.01 およびそれ以前)
・B/M9000 VP (R7.03.04 およびそれ以前)
・FieldMate (R1.01 および R1.02)

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

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おいて、意図的に細工された通信フレームを受信すると、通信機能が停止します。そして、その通信機能を有するプロセスが停止します。また 攻撃者によりこの脆弱性を利用され、該当プロセスを実行するシステム権限で他のプログラムが実行されるリスクがあります。

（参考）CVSS における本脆弱性の基本値は 10.0、現状値は 8.3 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)	

なお、影響を受ける製品が接続されているネットワークが他のネットワークと直接接続されていないなど、システム全体のネットワークが適切に管理されている場合、今回確認された脆弱性が悪用されるリスクは少ないと考えられます。

対策方法:

影響を受ける製品の最新リリースにて本脆弱性は基本的に修正されています。したがって、ソフトウェアを最新版にアップグレードいただくようお願いいたします。

直ちにソフトウェアを最新版にアップグレードすることが難しい場合は、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。

最新版へのアップグレード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。

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:

本脆弱性を有する機能は、オフィスネットワークとの通信では使用されるものではありません。そのため、オフィスネットワークと制御システムとの間にファイアーウォールを設置し適切なセキュリティ設定を施すことで、本脆弱性を利用した、オフィスネットワークからの攻撃に対する防御が可能となります。

また、影響を受ける製品が接続されているネットワークには不審な機器が接続されないよう、ネットワークを適切に管理されることを推奨します。

オフィスネットワーク経由以外のマルウェアの侵入経路として、USB メモリなどのリムーバブルメディアがあります。こ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。

ファイアーウォール設置および設定作業など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。

サポート:

本ドキュメントの内容に関する一般的なご質問や最新版の入手等については、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

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation

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:

2015-09-10:	初版
2017-03-30:	第 2 版:影響を受ける製品情報を更新
2017-12-22:	第 3 版:サポートの URL を更新

※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

All Rights Reserved. Copyright © 2015, Yokogawa Electric Corporation