Yokogawa Security Advisory Report

YSAR-19-0003

公開日 2019-9-27
最終更新日 2021-9-6

YSAR-19-0003: 横河製品が登録する Windows サービスで実行ファイルのパスが引用符で囲まれていない脆弱性

概要:

複数の横河製品で、アプリケーションが登録する Windows サービスの実行ファイルパスが引用符で囲まれていない脆弱性が存在することが判明しました。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。

- Exaopc (R3.01.00 - R3.77.00) *4
- Exaplog (R1.10.00 - R3.40.00)
- Exaquantum (R1.10.00 - R3.15.00) *1
- Exaquantum/Batch (R1.01.00 - R3.10.00) *2
- Exasmoc (全レビジョン)
- Exarqe (全レビジョン)
- GA10 (R1.01.01 - R3.05.01)
- InsightSuiteAE (R1.01.00 - R1.06.00)
- ProSafe-RS (R1.01.00 - R4.04.00)
- IA システム製品仮想化プラットフォーム (R1.01.00) *3
- PRM (R4.01.00 - R4.03.00)
- フィールド無線用 OPC サーバ (R2.01.00, R2.01.01, R2.01.03, R2.01.10)
- Exapilot (R1.01.00 - R3.98.10)
- STARDOM VDS (R4.01 - R8.10)
- STARDOM FCN/FCJ OPC サーバ for Windows (R1.01 - R4.20)

*1 Exaquantum R3.10.00 は影響なしと記載していましたが、影響を受けるレビジョンとなります
*2 Exaquantum/Batch R3.10.00 は修正された Rev として記載していましたが、影響を受けるレビジョンとなります
*3 Thin Client のみ影響を受けます
*4 形名、基本仕様コード: NTPF100-SX のみ影響を受けます

脆弱性詳細:

Windows サービスの実行ファイルパスに空白文字が含まれ、かつ引用符で囲まれていない場合に、空白文字を含むパスを利用して、当該サービスの権限で不正なファイルが実行される可能性があります。

CVSS v3 における本脆弱性の基本値は 8.4、現状値は 8.0 です。
AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

対策方法:

製品により対策が異なります。下記をご確認下さい。

製品名	影響を受けるレビジョン	対策方法
Exaopc (NTPF100-SX のみ)	R3.01.00 – R3.77.00	最新レビジョン(R3.78.00)へのレビジョンアップをご検討ください。 R3.78.00 で修正済みです。
Exaplog	R1.10.00 – R3.30.00	最新レビジョン(R3.40.00)へレビジョンアップの上、パッチ版(R3.40.06)適用をご検討ください。
	R3.40.00	パッチ版(R3.40.06)適用をご検討ください。
Exaquantum	R1.10.00 – R3.10.00	最新レビジョン(R3.20.00)へのレビジョンアップをご検討ください。 R3.20.00 で修正済みです。
	R3.15.00	パッチ版(R3.15.15)適用、または最新レビジョン(R3.20.00)へのレビジョンアップをご検討ください。
Exaquantum/Batch	R1.01.00 – R3.10.00	最新レビジョン(R3.10.10)へのレビジョンアップをご検討ください。 R3.10.10 で修正済みです。
Exasmoc	全レビジョン	2019/9/30 でサポート終了となります。 後継製品である Platform for Advanced Control and Estimation への乗り換えをご検討ください。
Exarqe	全レビジョン	2019/9/30 でサポート終了となります。 後継製品である Platform for Advanced Control and Estimation への乗り換えをご検討ください。
GA10	R1.01.01 – R3.05.01	最新レビジョン(R3.05.06)へのレビジョンアップをご検討ください。 R3.05.02 で修正済みです。
InsightSuiteAE	R1.01.00 – R1.06.00	最新レビジョン(R1.07.00)へのレビジョンアップをご検討ください。 R1.07.00 で修正済みです。
ProSafe-RS	R1.01.00 – R4.04.00	最新レビジョン(R4.05.00)へのレビジョンアップをご検討ください。 R4.05.00 で修正済みです。
IA システム製品仮想化プラットフォーム (Thin Client のみ)	R1.01.00	最新レビジョン(R1.01.10)へのレビジョンアップをご検討ください。 R1.01.10 で修正済みです。
PRM	R4.01.00 – R4.03.00	最新レビジョン(R4.04.00)へのレビジョンアップをご検討ください。 R4.04.00 で修正済みです。
フィールド無線用 OPC サーバ	R2.01.00, R2.01.01, R2.01.03, R2.01.10	パッチ版 R2.01.11 を適用してください
Exapilot	R1.01.00 – R3.98.10	最新レビジョン(R3.99.00)へのレビジョンアップをご検討ください。 R3.99.00 で修正済みです。
STARDOM VDS	R4.01 – R8.10	最新レビジョン(R9.01.01)へのレビジョンアップをご検討ください。 R9.01.01 で修正済みです。
STARDOM FCN/FCJ OPC サーバ for Windows	R1.01 – R4.20	最新レビジョン(R4.30.01)へのレビジョンアップをご検討ください。 R4.30.01 で修正済みです。

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。
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:

2019-9-27: 初版
2019-10-11: 影響を受ける製品、対策方法を更新(Exaquantum)
2019-10-24: 対策方法を更新(Exaquantum)
2019-11-1: 対策方法を更新(Exaquantum)
2020-1-24: 影響を受ける製品、対策方法に ProSafe-RS を追加
2020-6-26: 影響を受ける製品、対策方法に仮想化プラットフォームを追加、及び Exaquantum を更新
2020-7-31: Exaopc の対象 Rev を更新
2021-7-5: 影響を受ける製品、対策方法に PRM, フィールド無線用 OPC サーバを追加
2021-9-6: 影響を受ける製品、対策方法に Exapilot, STARDOM VDS, STARDOM FCN/FCJ OPC サーバ for Windows 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。