Yokogawa Security Advisory Report

YSAR-19-0001

公開日 2019-1-25
最終更新日 2019-1-25

YSAR-19-0001: 横河製品のライセンスマネージャーサービスにアクセス制御の脆弱性

概要:

横河製品のライセンスマネージャーサービスにアクセス制御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:

下記製品に脆弱性が存在します。

- CENTUM シリーズ
  - CENTUM VP (R5.01.00～R6.06.00)
  - CENTUM VP Small (R5.01.00～R6.06.00)
  - CENTUM VP Basic (R5.01.00～R6.06.00)
- ProSafe-RS (R3.01.00～R4.04.00)
- PRM (R4.01.00～R4.02.00)
- B/M9000 VP (R7.01.01～R8.02.03)

脆弱性詳細:

ライセンスマネージャーサービスが動作するコンピューターにおいて、リモートから当該サービスを実行するシステム権限で任意の場所に任意のファイルを作成／上書きできてしまいます。
攻撃者によりこの脆弱性を利用された場合、当該コンピューターの機能を妨害される等のリスクがあります。

CVSS v3 における本脆弱性の基本値は 8.1、現状値は 7.3 です。
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

対策方法:

下記パッチ版を適用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 VP CENTUM VP Small CENTUM VP Basic	R5.01.00～R5.04.00	R5.04.20 へのレビジョンアップと、R5.04.20 用パッチ版(R5.04.C5)適用をご検討ください。
	R5.04.20	R5.04.20 用パッチ版(R5.04.C5)を適用ください。
	R6.01.00～R6.05.00	R6.06.00 へのレビジョンアップと、R6.06.00 用パッチ版(R6.06.03)適用をご検討ください。
	R6.06.00	R6.06.00 用パッチ版(R6.06.03)を適用ください。
ProSafe-RS	R3.01.00～R3.02.10	R3.02.20 へのレビジョンアップと、R3.02.20 用パッチ版(R3.02.38)適用をご検討ください。
	R3.02.20	R3.02.20 用パッチ版(R3.02.38)を適用ください。
	R4.01.00～R4.03.10	R4.04.00 へのレビジョンアップと、R4.04.00 用パッチ版(R4.04.01)適用をご検討ください。
	R4.04.00	R4.04.00 用パッチ版(R4.04.01)を適用ください。
PRM	R4.01.00	R4.02.00 へのレビジョンアップと、R4.02.00 用パッチ版(R4.02.01)適用をご検討ください。
	R4.02.00	R4.02.00 用パッチ版(R4.02.01)を適用ください。
B/M9000 VP	R7.01.01～R8.02.03	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 VP が脆弱性の影響を受けるため、そちらをご確認ください。 CENTUM VP を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。

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。
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しています。

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:

横河電機は、本脆弱性の対応にご協力していただいた以下の方に感謝いたします。
・Segey Temnikov, Kaspersky Lab ICS CERT

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:

2019-1-25: 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。