Yokogawa Security Advisory Report

YSAR-18-0008

公開日 2018-12-21
最終更新日 2018-12-21

YSAR-18-0008: Vnet/IP オープン通信ドライバにサービス運用妨害(DoS)の脆弱性

概要:

Vnet/IP オープン通信ドライバに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 CS 3000 (R3.05.00～R3.09.50)
  - CENTUM CS 3000 Small (R3.05.00～R3.09.50)
  - CENTUM VP (R4.01.00～R6.03.10)
  - CENTUM VP Small (R4.01.00～R6.03.10)
  - CENTUM VP Basic (R4.01.00～R6.03.10)
- Exaopc (R3.10.00～R3.75.00)
- PRM (R2.06.00～R3.31.00)
- ProSafe-RS (R1.02.00～R4.02.00)
- FAST/TOOLS (R9.02.00～R10.02.00)
- B/M9000VP (R6.03.01～R8.01.90)

脆弱性詳細:

DoS 攻撃により Vnet/IP オープン通信ドライバの通信機能が停止する可能性があります。

CVSS v3 における本脆弱性の基本値は 7.5、現状値は 7.2 です。
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C

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 3000 CENTUM CS 3000 Small	R3.05.00～R3.09.50	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 へのアップグレードをご検討ください。
CENTUM VP CENTUM VP Small CENTUM VP Basic	R4 シリーズの全レビジョン	
	R5 シリーズの全レビジョン	Vnet/IP オープン通信ドライバ パッチ版 R10.01.08 を適用ください。
	R6.03.10 以前の R6 シリーズ	Vnet/IP オープン通信ドライバ パッチ版 R10.01.08 を適用ください。 R6.04.00 で修正済み。
Exaopc	R3.10.00～R3.60.00	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。最新のバージョン・レビジョンへのアップグレードをご検討ください。
	R3.70.00～R3.75.00	Vnet/IP オープン通信ドライバ パッチ版 R10.01.08 を適用ください。 R3.76.00 で修正済み。
PRM	R2.06.00～R3.04.00	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。最新のバージョン・レビジョンへのアップグレードをご検討ください。
	R3.05.00～R3.31.00	Vnet/IP オープン通信ドライバ パッチ版 R10.01.08 を適用ください。 R4.01.00 で修正済み。
ProSafe-RS	R1, R2 シリーズの全レビジョン	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。最新のバージョン・レビジョンへのアップグレードをご検討ください。
	R3 シリーズの全レビジョン	Vnet/IP オープン通信ドライバ パッチ版 R10.01.08 を適用ください。
	R4.02.00 以前の R4 シリーズ	Vnet/IP オープン通信ドライバ パッチ版 R10.01.08 を適用ください。 R4.03.00 で修正済み。
FAST/TOOLS	R9.02.00～R9.03.00	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。最新のバージョン・レビジョンへのアップグレードをご検討ください。
	R9.04.00～R9.05.00	Vnet/IP オープン通信ドライバ パッチ版 R10.01.08 を適用ください。
	R10.02.00 以前の R10 シリーズ	Vnet/IP オープン通信ドライバ パッチ版 R10.01.08 を適用ください。 R10.03.00 で修正済み。
B/M9000CS	-	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 は Vnet/IP を使用していません。
B/M9000 VP	R6.03.01～R8.01.90	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。

システムアップグレード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

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:

2018-12-21: 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。