

Yokogawa Security Advisory Report

YSAR-22-0005

公開日 2022-06-03
最終更新日 2022-07-27

YSAR-22-0005: ワイドエリアコミュニケーションルータにサービス運用妨害(DoS)の脆弱性

概要:

ワイドエリアコミュニケーションルータ (WAC ルータ) にサービス運用妨害 (DoS) の脆弱性が存在することを確認しました。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:

- ワイドエリアコミュニケーションルータ用通信モジュール (AW810D 用) VI461
影響を受けるレビジョン: Vnet/IP ファームウェア (F) R12 およびそれ以前

脆弱性詳細:

WAC ルータが不正なパケットによるサービス運用妨害 (DoS) 攻撃を受けた場合、WAC ルータの機能が停止する可能性があります。

- 不十分なランダム値の使用 ([CWE-330](#))

CVE: [CVE-2022-32284](#)

CVSS v3 基本値: 5.9

[CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H](#)

対策方法:

ワイドエリアコミュニケーションルータ用通信モジュール (AW810D 用) VI461

影響を受けるレビジョン	修正 Rev	対策方法
Vnet/IP ファームウェア (F) R12 およびそれ以前	R13	R13 以降へアップデートして下さい

横河は上記の対策方法に記載されている通り、アップデートを推奨します。

なお、Vnet/IP ファームウェアはお客様ではアップデートできません。

アップデートを希望する場合は、弊社営業またはサービス担当に Vnet/IP ファームウェアの更新を依頼してください。

アップデート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、アンチウイルス、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:

2022-06-03: 初版

2022-07-27: 第 2 版 : CVE 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。