Yokogawa Security Advisory Report

YSAR-26-0002

公開日 2026-02-13
最終更新日 2026-02-13

YSAR-26-0002: Vnet/IP インターフェースパッケージに複数の脆弱性

概要:
Vnet/IP インターフェースパッケージに複数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:
下記製品に脆弱性が存在します。

製品名	影響を受けるバージョン	影響を受ける製品に関連する横河製品(*2)
Vnet/IP インターフェースパッケージ(*1) (CENTUM VP R6 用 VP6C3300) (CENTUM VP R7 用 VP7C3300)	R1.07.00 以前	CENTUM VP R6, CENTUM VP R7

*1: Vnet/IP インターフェースパッケージは仮想化プラットフォーム上の横河製品が Vnet/IP 通信をする場合に必要となる製品です。
*2: 当該製品を仮想化プラットフォーム上に構築し、影響受ける製品を導入している場合に本レポートの脆弱性の影響を受けます。

脆弱性詳細 1:
影響を受ける製品が細工されたパケットを受信した場合、DoS 攻撃により Vnet/IP 通信機能が停止する、または、任意のプログラムが実行される可能性があります。

CWE-787 : 境界外書き込み
CWE-191 : 整数アンダーフロー
CVE: CVE-2025-1924
CVSS v3 基本値:6.9
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:H
CVSS v4 基本値: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:H/SC:N/SI:L/SA:L

脆弱性詳細 2:
影響を受ける製品が細工されたパケットを受信した場合、Vnet/IP ソフトスタックのプロセスを強制終了される可能性があります。

CWE-617 : 到達可能なアサーション
CVE: CVE-2025-48019
CVSS v3 基本値:5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4 基本値: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-617 : 到達可能なアサーション
CVE: CVE-2025-48020
CVSS v3 基本値:5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 基本値: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-191 : 整数アンダーフロー
CVE: CVE-2025-48021
CVSS v3 基本値:5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 基本値: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-130 : レングスパラメーターの不整合による不適切な処理
CVE: CVE-2025-48022
CVSS v3 基本値:5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 基本値: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-617 : 到達可能なアサーション
CVE: CVE-2025-48023
CVSS v3 基本値:5.3
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4 基本値: 6.0
CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

対策方法:

	影響を受けるレビジョン	修正 Rev	対策方法
Vnet/IP インターフェースパッケージ	R1.07.00 以前	R1.08.00	パッチ版(R1.08.00)を適用してください。

 # 本レポートで説明された脆弱性について
本レポートで説明された脆弱性は影響を受ける製品の不適合ではありません。
そのため、本レポートで説明された対策に関する作業を横河にご依頼いただいた場合、当該作業にかかる費用はお客様負担となります。

 # 対策についての推奨事項
サイバーセキュリティリスクの低減のために、横河は本レポートで説明された対策の適用を推奨します。
なお本レポートで報告されている脆弱性の実際の影響度は、各お客様固有のシステム環境によって異なります。お客様が本レポートを参考に、本レポートで説明された対策を適用するかどうか、いつ適用するか等について判断される事を推奨します。

横河では本レポートで説明された対策の適用に関するご相談、および各種セキュリティ対策についてのご相談も承っています。詳細な情報または支援が必要な場合は、弊社サービス拠点までお問い合わせください。

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:
本脆弱性は以下の方々により発見・通知されました。
- Dmitry Sklyar (Positive Technologies) for CVE-IDs: CVE-2025-1924, CVE-2025-48019, CVE-2025-48020, CVE-2025-48023
- Demid Uzenkov (Positive Technologies) for CVE-IDs: CVE-2025-1924, CVE-2025-48021, CVE-2025-48022

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
   https://www.first.org/cvss/
   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:
2026-02-13: 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。