

# Cisco AppDynamics Network Visibility ServiceのDoS脆弱性



アドバイザーID : cisco-sa-appd-netvisdos-9zNbsJtK

[CVE-2024-20394](#)

初公開日 : 2024-05-15 16:00

バージョン 1.0 : Final

CVSSスコア : [5.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwh65251](#)

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

## 概要

Cisco AppDynamics Network Visibility Agentの脆弱性により、認証されていないローカル攻撃者が該当デバイスでサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、予期しない入力を処理できないことに起因します。ローカルデバイスにアクセスできる攻撃者は、標的となるサービスにHTTP要求を送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はローカルデバイスでNetwork Agent Serviceを停止することにより、DoS状態を引き起こすことができます。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

このアドバイザーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-netvisdos-9zNbsJtK>

## 該当製品

### 脆弱性のある製品

公開時点では、この脆弱性はCisco AppDynamics Network Visibility Agentに影響を与えていました。

公開時点で脆弱性が確認されている Cisco ソフトウェアのリリースについては、このアドバイザーの「修正済みソフトウェア」セクションを参照してください。最も完全で最新の情報については、このアドバイザーの上部にあるバグ ID の詳細セクションを参照してください。

## 脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

## 回避策

この脆弱性に対処する回避策はありません。

## 修正済みソフトウェア

シスコのAppDynamicsは、このアドバイザリに記載された脆弱性に対処するためのソフトウェアアップデートをリリースしました。お客様がインストールしたり、サポートを受けたりできるのは、最新のライセンスを保持し、有効なサポートとメンテナンス契約を持つソフトウェアバージョンとフィーチャセットのみです。このようなソフトウェアアップグレードをインストール、ダウンロード、アクセス、またはその他の方法で使用するにより、お客様はAppDynamicsのライセンス契約の条項に従うことに同意したことになります。セキュリティソフトウェアアップデートによって、お客様に新しいソフトウェアライセンスや追加のソフトウェアフィーチャセットに対する権限が付与されることはありません。

有効なサポートおよびメンテナンス契約を持つ最新ライセンスをお持ちのお客様は、既存のAppDynamics配信サーバーのダウンロードアカウントからソフトウェアの修正バージョンをダウンロードできます。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。情報が不明な場合は、AppDynamicsサポートシステムでサポートチケットを開くことをお勧めします。

## 修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列にはCisco AppDynamicsソフトウェアリリースが、右の列にはリリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースが示されています。

Cisco AppDynamicsネットワーク可視性エージェント	First Fixed Release (修正された最初のリリース)
24.3.0 以前	24.4.0

修正済みリリースは、AppDynamicsソフトウェアポータル(<https://download.appdynamics.com>)が

ら入手できます。修正済みソフトウェアをダウンロードするには、お客様にAppDynamicsアカウントが必要です。

Product Security Incident Response Team ( PSIRT; プロダクト セキュリティ インシデント レスポンス チーム ) は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

## 不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

## 出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-netvisdos-9zNbsJtK>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2024年5月15日

## 利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。