Cisco ThousandEyes Enterprise Agentの任意のファイル上書きの脆弱性

Medium

アドバイザリーID : cisco-sa-te-agentfilewrite-tqUw3SMU
初公開日 : 2026-04-15 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 : CSCwt47572

CVE-2026-20161

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 ThousandEye Enterprise AgentのCLIの脆弱性により、権限の低い認証されたローカル攻撃者が、該当デバイスのローカルシステム上で任意のファイルを上書きできるようになります。

この脆弱性は、該当デバイスのローカルファイルシステムにあるファイルのアクセス制御が不適切なことに起因します。攻撃者は、ローカルファイルシステムの特定の場所にシンボリックリンクを配置することにより、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、攻撃者はファイルシステムの権限をバイパスし、該当デバイスの任意のファイルを上書きできるようになります。

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。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-agentfilewrite-tqUw3SMU

該当製品

脆弱性のある製品

公開時点では、デバイス設定に関係なく、この脆弱性はCisco ThousandEyes Enterprise Agent Linuxパッケージのインストールタイプに影響を与えました。

このアドバイザリの公開時点で脆弱性が存在するシスコソフトウェアリリースについては、このアドバイザリの「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。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- ThousandEyes仮想アプライアンスのインストールタイプ
- Dockerを搭載したCiscoルータ上のThousandEyesエンタープライズエージェント
- ThousandEyes Docker イメージをインストールした場合

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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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。

左側の列にはシスコソフトウェアリリース、右側の列にはリリースがこのアドバイザリに記載されている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 ThousandEyes Enterprise Agent リリース	First Fixed Release（修正された最初のリリース）
1.2 以前	1.234.0

Cisco ThousandEyes Enterprise 仮想アプライアンスで Ubuntu Linux サーバーが実行され、無人アップグレードパッケージがデフォルトでインストールされているため、すべての重要なセキュリティ修正が自動的にインストールされます。無人アップグレードには、インターネットと Ubuntu リポジトリへのアクセスが必要です。

シスコの 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済み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

この脆弱性を報告していただいたセキュリティ研究者のDevin Wittmayer氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-agentfilewrite-tqUw3SMU

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	2026年4月15日

利用規約

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。