# Cisco ThousandEyesエージェントの証明書検証の脆弱性

Medium

アドバイザリーID : cisco-sa-thousandeyes-cert-pqtJUv9N
CVE-2025-20126
初公開日 : 2025-01-08 16:00
最終更新日 : 2025-01-08 18:35
バージョン 1.1 : Final
CVSSスコア : 4.8
回避策 : No workarounds available
Cisco バグ ID : CSCwm51243

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 Endpoint Agent for macOSおよびRoomOSの認証検証ルーチンにおける脆弱性により、認証されていないリモートの攻撃者がメトリック情報を傍受または操作する可能性があります。

この脆弱性は、影響を受けるソフトウェアがホステッドメトリックサービスの証明書を適切に検証していないことに起因します。パス上の攻撃者は、巧妙に細工された証明書を使用してネットワークトラフィックを傍受することにより、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、攻撃者は信頼できるホストになりすまして、リモートメトリックサービスと脆弱なクライアント間の通信を監視または変更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-thousandeyes-cert-pqtJUv9N

## 該当製品

### 脆弱性のある製品

公開時点で、デバイスの設定にかかわらず、Cisco ThousandEyes Endpoint Agentソフトウェアの脆弱性のあるリリースを実行しているCisco ThousandEyes Endpoint Agent for macOSと

RoomOSは、この脆弱性の影響を受けました。

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

シスコは、この脆弱性がWindows用Cisco ThousandEyesエンドポイントエージェントには影響を与えないことを確認しました。

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。

## 回避策

この脆弱性に対処する回避策はありません。ただし、管理者は、該当するソフトウェアバージョンでの脆弱性の不正利用を防ぐために、エージェントインスタントテスト機能を無効にすることができます。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

## 修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

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。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

### 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。

| Platform | 最初の修正Cisco ThousandEyes Agentリリース |
|---|---|
| MacOS | 1.206.3 |
| ルームOS | 1.207.21 |

1. 更新されたエージェントを含む最初のRoomOSリリースは、RoomOSリリース11.22.1.0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

この脆弱性は、シスコのKonrad Porzezynskiが社内セキュリティテストで発見しました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thousandeyes-cert-pqtJUv9N

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.1 | 影響を受けないエージェントのバージョンに関する情報を更新し、古いバージョンのエージェントに対する緩和策を追加。 | 脆弱性が存在しない製品と回避策 | Final | 2025年1月8日 |
| 1.0 | 初回公開リリース | — | Final | 2025年1月8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、単独の転載や意訳を施した場合、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。