

Cisco Catalyst SD-WAN Managerの証明書検証の脆弱性



アドバイザリーID : cisco-sa-catalyst-tls-PqnD5KEJ [CVE-2025-20157](#)
初公開日 : 2025-05-07 16:00
バージョン 1.0 : Final
CVSSスコア : [5.9](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCwm84885](#)

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 Catalyst SD-WAN Manager (旧称Cisco SD-WAN vManage) の証明書検証処理の脆弱性により、認証されていないリモートの攻撃者が機密情報にアクセスできる可能性があります。

この脆弱性は、Smart Licensing機能で使用する証明書の検証が不適切なことに起因します。ネットワーク上に特権を持つ攻撃者は、インターネット経由で送信されるトラフィックを傍受することで、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、デバイスがシスコクラウドサービスに接続するために使用するクレデンシャルなどの機密情報にアクセスできる可能性があります。

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-catalyst-tls-PqnD5KEJ>

該当製品

脆弱性のある製品

この脆弱性は、発行時点で、シスコがホストするSmart Licensingサービスに接続するように設定されているCisco Catalyst SD-WAN Managerに影響を与えました。

このアドバイザリー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、このアドバイザリの上にあるバグ 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。

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

[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

このアドバイザリは、Cisco Catalyst SD-WAN Managerの脆弱性に関する一連のアドバイザリの一部です。このコレクションには、次のアドバイザリが含まれます。

- [Cisco Catalyst SD-WAN Managerの特権昇格の脆弱性](#)
- [Cisco Catalyst SD-WAN Managerの任意のファイル作成の脆弱性](#)
- [Cisco Catalyst SD-WAN Managerの証明書検証の脆弱性](#)
- [Cisco Catalyst SD-WAN Managerの任意のファイルを上書きする脆弱性](#)
- [Cisco Catalyst SD-WAN Managerストアのクロスサイトスクリプティングの脆弱性](#)
- [Cisco Catalyst SD-WAN Managerの反映HTMLインジェクションの脆弱性](#)

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にあるバグ ID の詳細セクションを参照してください。

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、および、この脆弱性に対する修正を含む最初のリリースを示しています。右の列は、リリースがこのアドバイザリ集の一部である脆弱性の影響を受けるかどうか、およびこのコレクションのすべての脆弱性に対する修正を含むリリースを示しています。

該当する修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Catalyst SD-WAN Managerリリース	この脆弱性に対する最初の修正リリース	このコレクションに含まれるすべての脆弱性に対する最初の修正リリース
20.8以前 ¹	修正済みリリースに移行。 。	修正済みリリースに移行。
20.92	20.9.7	修正済みリリースに移行。
20.101	修正済みリリースに移行。 。	修正済みリリースに移行。
20.111	修正済みリリースに移行。 。	修正済みリリースに移行。
20.12	20.12.5	修正済みリリースに移行。
20.131	修正済みリリースに移行。 。	修正済みリリースに移行。
20.142	修正済みリリースに移行。 。	修正済みリリースに移行。
20.15	20.15.2	修正済みリリースに移行。
20.16	脆弱性なし	20.16.1

1. これらのリリースは [ソフトウェアメンテナンスが終了](#)しています。シスコでは、お客様が [サポートされているリリースにアップグレード](#)することを強く推奨します。
2. これらのリリースは、サポート終了プロセスに入っています。特定のリリースのマイルストーン日付については、そのリリースの『[販売終了およびサポート終了のお知らせ](#)』を参照してください。

ソフトウェアの移行を検討する際は、[シスコ セキュリティ アドバイザリ (Cisco Security Advisories)] 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の有無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、新しいソフトウェアがお客様のネットワークニーズに十分に対応し、現在のハードウェアおよびソフトウェア構成が新しい製品で適切にサポートされ続けることを確認する必要があります。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。

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-catalyst-tls-PqnD5KEJ>

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	2025年5月7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。