Cisco Catalyst SD-WAN Managerの情報開示の脆弱性

Medium

アドバイザリーID : cisco-sa-sdwan-infodis-SPuJBDCe
CVE-2026-20294
初公開日 : 2026-08-05 16:00
最終更新日 : 2026-08-07 21:26
バージョン 1.1 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwu18179

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のWebベース管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、該当システムで機密情報をクリアテキストで表示できるようになります。

この脆弱性は、暗号化の許可リストに含まれていない特定のテンプレートタイプに対するアクセスコントロールの適用が不十分であることに起因します。権限の低い攻撃者が、ローカルシステムまたはリモートロギングサーバでログを表示することにより、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、攻撃者は機密性の高い認証クレデンシャルを表示し、ネットワークインフラストラクチャと接続サービスのさらなる侵害につなが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-sdwan-infodis-SPuJBDCe

該当製品

脆弱性のある製品

公開時点では、デバイスの設定にかかわらず、この脆弱性はCisco Catalyst SD-WAN

Managerに影響を与えていました。

この脆弱性は、次を含むすべての導入タイプに影響を与えました。

- オンプレミス展開
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WAN Cloud（Cisco Managed）
- 政府/自治体向け Cisco SD-WAN（FedRAMP）

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。

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 Catalyst SD-WAN リリース	First Fixed Release（修正された最初のリリース）
20.91 より前	修正済みリリースに移行。
20.9	20.9.10

Cisco Catalyst SD-WAN リリース	First Fixed Release（修正された最初のリリース）
20.10	20.12.8
20.111	20.12.8
20.12	20.12.8
20.131	20.15.6
20.141	20.15.6
20.15	20.15.6
20.161	20.18.4
20.18	20.18.4
26.1	26.1.2
26.2	26.2.1

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、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。

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。

シスコは、クラウドベースの Cisco SD-WAN Cloud（Cisco Managed）リリース 20.15.602 においても、この脆弱性に対処しています。ユーザの対処は必要ありません。サービス GUI のヘルプ機能を使用すると、現在の修復ステータスやソフトウェアバージョンを確認できます。

その他の情報が必要な場合は、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。

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

シスコは、この脆弱性を報告していただいた米国サイバーセキュリティおよびインフラストラクチャセキュリティ機関(CISA)のStephen Thurston氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-SPuJBDCe

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	Cisco SD-WAN Cloud(Cisco Managed)リリース 20.15.602に関する情報を追加。	修正済みリリース	Final	2026年8月7日
1.0	初回公開リリース	—	Final	2026年8月5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。