Cisco Secure Network Analyticsの特権昇格の脆弱性

Medium

アドバイザリーID : cisco-sa-sna-prvesc-4BQmK33Z
初公開日 : 2025-04-16 16:00
バージョン 1.0 : Final
CVSSスコア : 6.0
回避策 : No workarounds available
Cisco バグ ID : CSCwn51215

CVE-2025-20178

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 Secure Network AnalyticsのWebベースの管理インターフェイスにおける脆弱性により、有効な管理クレデンシャルを持つ認証されたリモートの攻撃者が、基盤となるオペレーティングシステムでルートとして任意のコマンドを実行できる可能性があります。

この脆弱性は、デバイスのバックアップファイル内の整合性チェックが不十分であることに起因します。有効な管理者クレデンシャルを持つ攻撃者は、悪意のあるバックアップファイルを作成して該当デバイスに復元することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者はルートの権限を使用して、基盤となるオペレーティングシステムにシェル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-sna-prvesc-4BQmK33Z

該当製品

脆弱性のある製品

公開時点では、この脆弱性はデバイス設定に関係なく、次のシスコ製品に影響を与えていました。

- Secure Network Analyticsデータストア

- Secure Network Analyticsフローコレクタ
- Secure Network Analyticsフローセンサー
- Secure Network Analytics Manager
- Secure Network Analytics UDP Director
- Secure Network Analytics Virtual Data Store
- Secure Network Analytics Virtual Flow Collector
- Secure Network Analytics Virtual Flow Sensor
- Secure Network Analytics Virtual Manager
- Secure Network Analytics Virtual UDP Director

注：Cisco Secure Network Analyticsリリース7.5.0より前のリリースでは、デフォルトでシステム管理者(sysadmin)ルートシェルアクセスが許可されており、この脆弱性の影響を受けません。詳細については、『Cisco Secure Network Analytics Systemコンフィギュレーションガイド』を参照してください。

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。このアドバイザリの先頭にあるバグIDの詳細情報のセクションで、最新の情報を確認してください。

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Cisco Secure Cloud Analyticsには影響を与えないことを確認しました。

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

発行時点では、次の表に示すリリース情報は正確でした。このアドバイザリの先頭にあるバグIDの詳細情報のセクションで、最新の情報を確認してください。

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 Secure Network Analytics のリリース	First Fixed Release（修正された最初のリリース）
7.4 以前	脆弱性なし
7.5.0	7.5.0 ROLLUP20250218-01
7.5.1	7.5.1 ROLLUP20250218-01
7.5.2	7.5.2 ROLLUP20250319-01

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

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-sna-prvesc-4BQmK33Z

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4月16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。