

Cisco Secure ClientソフトウェアのDoS脆弱性



アドバイザリーID : cisco-sa-accsc-dos-9SLzkZ8

[CVE-2023-20241](#)

初公開日 : 2023-11-15 16:00

[CVE-2023-](#)

バージョン 1.0 : Final

[20240](#)

CVSSスコア : [5.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwf21381](#) [CSCwf92553](#)

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 Clientソフトウェアの複数の脆弱性 (以前のAnyConnectセキュアモバイルクライアント) により、認証されたローカル攻撃者が該当システムにサービス妨害(DoS)状態を引き起こす可能性があります。

これらの脆弱性は、Cisco Secure Clientソフトウェアからの範囲外のメモリ読み取りに起因します。攻撃者は、別のユーザが同じシステム上のCisco Secure Clientにアクセスすると同時に該当デバイスにログインし、巧妙に細工されたパケットをそのローカルホスト上のポートに送信することで、これら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VPNエージェントサービスをクラッシュさせ、システムのすべてのユーザがサービスを利用できなくなる可能性があります。これらの脆弱性をエクスプロイトするには、攻撃者がマルチユーザシステムで有効なクレデンシャルを持っている必要があります。

シスコはこれら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。これら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-accsc-dos-9SLzkZ8>

注 : シスコポートフォリオの簡素化の一環として、セキュリティ製品の名称を変更し、Cisco Secure というブランド名に統一しています。詳細については、「[Cisco Secure が登場](#)」を参照してください。

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性は、次のシスコ製品で脆弱性が存在するソフトウェアリリースを実行している場合に影響を受けました。

- Android向けセキュアクライアントAnyConnect
- iOS用のセキュアなクライアントAnyConnect VPN
- ユニバーサルWindowsプラットフォーム用のセキュアクライアント (AnyConnectを含む)
- Secure Client for Linux (ダウンロード)
- MacOS用のセキュアクライアント

公開時点で脆弱性が確認されている Cisco ソフトウェアの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冒頭にあるバグIDの詳細情報の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記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。](#)

回避策

これら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アップグレードソリューション一式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にあるバグ ID の詳細セクションを参照してください。

左の列にはCiscoソフトウェアリリースがリストされ、中央と右の列には、そのリリースが本アドバイザリに記載された脆弱性の影響を受けるかどうかと、これら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 Clientソフトウェアリリース	CSCwf21381の最初の修正済みリリース	CSCwf92553の最初の修正済みリリース
4.10以前 ¹	4.10 MR8 (2023年12月)	4.10 MR8 (2023年12月)
5.0	5.0 MR4(5.0.04032)	5.0 MR5(5.0.05040)
5.1	脆弱性なし	脆弱性なし

1. Cisco Secure Clientソフトウェアリリース4.10以前は、Cisco AnyConnectセキュアモバイルクライアントと呼ばれていました。

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とその公表は確認しておりません。

出典

この脆弱性は、シスコ内部でのシステム 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-accsc-dos-9SLzkZ8>

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	2023-NOV-15

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。