

ISEポスチャモジュールを使用したCisco Secure Client for Linuxにおける権限昇格の脆弱性



アドバイザリーID : cisco-sa-secure-privesc-sYxQO6ds

[CVE-2024-20338](#)

初公開日 : 2024-03-06 16:00

バージョン 1.0 : Final

CVSSスコア : [7.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwi30539](#)

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 for LinuxのISEポスチャ (システムスキャン) モジュールの脆弱性により、認証されたローカルの攻撃者が該当デバイスの特権を昇格できる可能性があります。

この脆弱性は、制御されていない検索パス要素の使用に起因します。攻撃者は、悪意のあるライブラリファイルをファイルシステム内の特定のディレクトリにコピーし、管理者に特定のプロセスの再起動を促すことで、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root権限を使用して該当デバイスで任意のコードを実行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-secure-privesc-sYxQO6ds>

該当製品

脆弱性のある製品

この脆弱性は、Cisco Secure Client for Linuxの脆弱性が存在するリリースを実行し、ISEポスチャモジュールがインストールされているシスコデバイスに影響を与えます。

注:ISEポスチャモジュールをVPNポスチャ (ホストスキャンまたはセキュアファイアウォールポスチャ) モジュールと混同しないでください。VPNポスチャモジュールはこの脆弱性の影響

を受けません。

脆弱性が存在する Cisco 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。

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、この脆弱性の影響を受けることが分かっています。](#)

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- VPNポスチャモジュールのみがインストールされたSecure Client for Linux
- MacOS用のセキュアクライアント
- iOS、Android、ユニバーサルWindowsプラットフォームなどのモバイルデバイスのオペレーティングシステム用のSecure Client
- Secure Client for Windowsの場合

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャンネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェアバージョンとフィーチャセットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンスアップグレードです。無償のセキュリティソフトウェアアップデートによって、お客様に新しいソフトウェアライセンス、追加ソフトウェアフィーチャセット、またはメジャーリビジョンアップグレードに対する権限が付与されることはありません。

Cisco.com の [シスコサポート & ダウンロードページ](#)には、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス (My Devices)] ツールを使用するお客

様のカスタマーデバイスサポート範囲も表示できます。

[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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC (https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表に示すように、該当する修正済みのソフトウェア リリースにアップグレードすることをお勧めします。

Cisco Secure Client for Linuxリリース	First Fixed Release (修正された最初のリリース)
5.1.2.42 より前	5.1.2.42

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

この脆弱性を報告していただいたWargaming社のIvan Agarkov氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure->

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	2024年3月6日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。