VPN ポスチャ（HostScan）モジュール共有ライブラリを搭載した Linux および MacOS 用の CiscoAnyConnect セキュア モビリティ クライアントで確認されたハイジャック脆弱性。

High

アドバイザリーID : cisco-sa-anyconnect-lib-hija-cAFB7x4q
CVE-2021-34788
初公開日 : 2021-10-06 16:00
バージョン 1.0 : Final
CVSSスコア : 7.0
回避策 : No workarounds available
Cisco バグ ID : CSCvz38781

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

Linux および MacOS 用の CiscoAnyConnect セキュア モビリティ クライアントの共有ライブラリロードメカニズムの脆弱性により、VPN ポスチャ（HostScan）モジュールが AnyConnect にインストールされている場合、認証されたローカルの攻撃者が該当デバイスに対して共有ライブラリハイジャック攻撃を実行する可能性があります。

この脆弱性は、該当デバイスにロードされた共有ライブラリファイルの署名検証プロセスで競合状態が発生することに起因します。一連の細工されたプロセス間通信（IPC）メッセージが AnyConnect プロセスに送信されると、この脆弱性がエクスプロイトされ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、該当デバイスでルート権限を使用して任意のコードを実行できる可能性があります。この脆弱性をエクスプロイトするには、攻撃者はシステムに有効なアカウントを持っている必要があります。

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-anyconnect-lib-hija-cAFB7x4q

該当製品

脆弱性のある製品

この脆弱性は、VPN ポスチャ（HostScan）モジュールがインストールされている場合、Linux および MacOS 用の CiscoAnyConnect セキュア モビリティ クライアントの脆弱なリリースを実行しているデバイスに影響します。

注：VPNポスチャ(HostScan)モジュールをISEポスチャ(SystemScan)モジュールと混同しないでください。ISE 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。

- 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 オペレーティング システム用の AnyConnect セキュア モビリティ クライアント
- ISE ポスチャ（SystemScan）モジュールのみがインストールされた Linux および MacOS 用の AnyConnect セキュア モビリティ クライアント
- Windows 用 AnyConnect セキュア モビリティ クライアント

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。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ます。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。

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。

Linux および Mac OS リリース用の CiscoAnyConnect セキュア モビリティ クライアント	First Fixed Release（修正された最初のリリース）
4.10.03104 より前	4.10.03104

Cisco.com の Software Center からこのソフトウェアをダウンロードするには、次の手順を実行します。

1. [すべてを参照（Browse All）] をクリックします。
2. [セキュリティ（Security）] > [VPN およびエンドポイント セキュリティ クライアント（VPN and Endpoint Security Clients）] > [AnyConnect セキュア モビリティ クライアント（AnyConnect Secure Mobility Client）] > [AnyConnect セキュア モビリティ クライアント v4.x（AnyConnect Secure Mobility Client v4.x）] の順に選択します。
3. [AnyConnect セキュア モビリティ クライアント v4.x（AnyConnect Secure Mobility Client v4.x] ページの左側のペインからリリースを選択します。

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

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-anyconnect-lib-hija-cAFB7x4q

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	2021-OCT-06

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。