Windows 向け Cisco AnyConnect セキュア モビリティ クライアントの DLL および実行ファイルのハイジャックに対する脆弱性

High

アドバイザリーID : cisco-sa-anyconnect-code-exec-jR3tWTA6
初公開日 : 2021-05-05 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 : CSCvu77671 CSCvw18595 CSCvv43102 CSCvw17005 CSCvv60844 CSCvw18527 CSCvw16996

CVE-2021-1430
CVE-2021-1496
CVE-2021-1427
CVE-2021-1426
CVE-2021-1429
CVE-2021-1428

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

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのインストール、アンインストール、およびアップグレードプロセスに複数の脆弱性があるため、認証されているローカルの攻撃者がこのアプリケーションで使用される DLL および実行ファイルをハイジャックする可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスで SYSTEM 特権を使用して任意のコードを実行す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 Windows システムで有効なログイン情報を持っている必要があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

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-code-exec-jR3tWTA6

該当製品

脆弱性のある製品

これらの脆弱性は、Windows 向け Cisco AnyConnect 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シスコ デバイスに影響します。

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、これら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、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- Linux 用 AnyConnect セキュア モビリティ クライアント
- Mac OS 向け AnyConnect セキュア モビリティ 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 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

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

これらの脆弱性の詳細については、次のとおりです。

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのアンインストール実行ファイルのハイジャックに対する脆弱性

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのアンインストールプロセスの脆弱性により、認証されているローカルの攻撃者が該当デバイスで実行ファイル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、アンインストールプロセス中に安全でないアクセス許可を設定された一時ファイルが作成されるために発生します。攻撃者は、一時ファイルが実行のためにアクセスされる前にファイルを上書きすることで、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、攻撃者は該当デバイスで SYSTEM 特権を使用して任意のコードを実行す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 Windows システムで有効なログイン情報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。

バグID:CSCvv43102、CSCvv60844
CVE ID:CVE-2021-1426
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.0
CVSSベクトル：CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのアップグレード DLL のハイジャックに対する脆弱性

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのアップグレードプロセスに関する 2 つの脆弱性により、認証されているローカルの攻撃者が該当デバイスで DLL ハイジャック攻撃を実行する可能性があります。

これらの脆弱性は、アプリケーションが、ユーザが書き込み可能なディレクトリから DLL ファイルをロードするために発生します。攻撃者は、悪意のある DLL ファイルを特定のディレクトリにコピーすることで、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、攻撃者は該当デバイスで SYSTEM 特権を使用して任意のコードを実行す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 Windows システムで有効なログイン情報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。

バグID:CSCvw16996、CSCvw17005
CVE ID:CVE-2021-1427、CVE-2021-1428
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.0
CVSSベクトル：CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのアップグレード実行ファイルのハイジャックに対する脆弱性

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのインストールプロセスの脆弱性により、認証されているローカルの攻撃者が該当デバイスで実行ファイル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、アップグレードプロセス中に安全でないアクセス許可を設定された一時ファイルが作成されるために発生します。攻撃者は、一時ファイルが実行のためにアクセスされる前にファイルを上書きすることで、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、攻撃者は該当デバイスで SYSTEM 特権を使用して任意のコードを実行す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 Windows システムで有効なログイン情報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。

バグID:CSCvw18527
CVE ID:CVE-2021-1429
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.0
CVSSベクトル：CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのアップグレード DLL のハイジャックに対する脆弱性

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのアップグレードプロセスに関する脆弱性により、認証されているローカルの攻撃者が該当デバイスで DLL 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、アップグレードプロセス中に安全でないアクセス許可を設定された一時ファイルが作成されるために発生します。攻撃者は、一時ファイルが実行のためにアクセスされる前にファイルを上書きすることで、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、攻撃者は該当デバイスで SYSTEM 特権を使用して任意のコードを実行す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 Windows システムで有効なログイン情報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。

バグID:CSCvw18595
CVE ID:CVE-2021-1430
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.0
CVSSベクトル：CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのインストール実行ファイルのハイジャックに対する脆弱性

Windows 向け Cisco AnyConnect セキュア モビリティ クライアントのインストールプロセスの脆弱性により、認証されているローカルの攻撃者が該当デバイスで実行ファイル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、アプリケーションが、ユーザが書き込み可能なディレクトリから実行ファイルをロードするために発生します。攻撃者は、悪意のある実行ファイルを特定のディレクトリにコピーすることで、この脆弱性をエクスプロイトする可能性があります。コピーされたファイルは、アプリケーションのインストール時またはアップグレード時に実行されます。エクスプロイトに成功すると、攻撃者は該当デバイスで SYSTEM 特権を使用して任意のコードを実行する可能性

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 Windows システムで有効なログイン情報が必要になります。

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。

バグID:CSCvu77671
CVE ID:CVE-2021-1496
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.0
CVSSベクトル：CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

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

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

次の表で、左の列はこのアドバイザリで言及されている脆弱性の CVE 識別子を示しています。中央の列は、脆弱性の影響を受けるソフトウェアリリースを示しています。右側の列は、この脆弱性を修正した最初のリリースを示しています。このセクションの表に記載されている適切な修正済み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。

CVE 識別子	該当する Cisco AnyConnect リリース Windows 向けセキュア モビリティ クライアント	この脆弱性に対する最初の修正リリース
CVE-2021-1426	4.9.06037 より前	4.9.06037
CVE-2021-1427	4.9.06037 より前	4.9.06037
CVE-2021-1428	4.10.00093 より前	4.10.00093
CVE-2021-1429	4.10.00093 より前	4.10.00093
CVE-2021-1430	4.9.06037 より前	4.9.06037
CVE-2021-1496	4.9.03022 より前	4.9.03022

Cisco.com の Software Center から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）] > [Cisco VPN 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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

出典

シスコ は、これらの脆弱性を報告してくださった次の方々に感謝いたします。

- CVE-2021-1426：北京大学ワンスアンエ科大学のCan Huang氏とXinhui Han氏、デンマークのCyber DefenseのLasse Trolle Borup氏
- CVE-2021-1427:PwCルクセンブルクのサイバーセキュリティチームのLockheed Martin Redチームと Antoine Goichot
- CVE-2021-1428、CVE-2021-1429、CVE-2021-1430、およびCVE-2021-1496:Lockheed Martin Red Team

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-code-exec-jR3tWTA6

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 年 5 月 5 日

利用規約

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。