Windows 用 Cisco AnyConnect セキュアモビリティ DLL ハイジャックの脆弱性

High

アドバイザリーID : cisco-sa-anyconnect-dll-F26WwJW
CVE-2020-3433
初公開日 : 2020-08-05 16:00
最終更新日 : 2022-10-25 13:15
バージョン 1.2 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCvu14943

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 用 Cisco AnyConnect セキュア モビリティ クライアントのプロセス間通信（IPC）チャネルの脆弱性により、認証されたローカルの攻撃者が 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 システムで有効なクレデンシャルを持っている必要があります。

この脆弱性は、実行時にアプリケーションによって読み込まれるリソースの検証が不十分であることが原因です。攻撃者は巧妙に細工された IPC メッセージを AnyConnect プロセスに送信することにより、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、攻撃者は対象マシンで 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-dll-F26WwJW

該当製品

脆弱性のある製品

この脆弱性は、リリース 4.9.00086 より以前の Windows 用 Cisco AnyConnect セキュア モビリティ クライアント リリースに影響します。

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。

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

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 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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

シスコは、Windows 用 Cisco AnyConnect セキュア モビリティ クライアント リリース 4.9.00086 以降のこの脆弱性を修正しました。

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）は、このアドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイトコードが入手可能であることを認識しています。

2022 年 10 月、Cisco PSIRT は、これらの脆弱性のさらなるエクスプロイトが試みられたことを認識しました。これらの脆弱性が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、引き続き強くお勧めします。

出典

この脆弱性を報告してくださった PwC Luxembourg サイバーセキュリティチームの Antoine Goichot 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	シスコがアクティブなエクスプロイトの試みを認識したため、[エクスプロイト事例と公式発表] セクションを更新。	不正利用事例と公式発表	Final	2022 年 10 月 25 日
1.1	コンセプト実証エクスプロイトコードが利用可能であることを記載	不正利用事例と公式発表	Final	2020 年 8 月 13 日
1.0	初回公開リリース	—	Final	2020 年 8 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。