Cisco AnyConnect セキュア モビリティ クライアントの多重 脆弱点

severity

アドバイザリーID : cisco-sa-20110601-ac

初公開日 : 2011-06-01 16:00

バージョン 2.0 : Final

回避策 : Yes

Cisco バグ ID :

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

以前に Cisco AnyConnect VPN Client として知られている Cisco AnyConnect セキュア モビリティ クライアントは、次の脆弱性から影響を受けます:

- 任意 プログラムの実行脆弱性
- ローカル特権 拡大脆弱性

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 このアドバイザリに記載されている脆弱性に対する回避策はありません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110601-ac で掲示されます。

影響を受ける製品

脆弱性が存在する製品

この文書に説明がある脆弱性は Cisco AnyConnect セキュア モビリティ クライアントに適用します。 該当するバージョンは次のとおりです。

脆弱性	プラットフォーム	該当するバージョン
任意 プログラムの実行脆弱性	Microsoft Windows	2.3.185 以前のすべてのバージョン
	Linux、Apple MacOS X	• 2.5.x および 3.0.x 以外のメジャーリリースのすべてのバージョン。 • 2.5.3041 以前の 2.5.x リ

		リース • 3.0.629 以前の 3.0.x リリース
ローカル特権拡大脆弱性	Microsoft Windows	2.3.254 以前のすべてのバージョン
	Linux、Apple MacOS X	Not affected

注: Microsoft ウィンドウ モービル バージョンは任意 プログラムの実行脆弱性から影響を受けます。 Windows Mobile のための Cisco AnyConnect セキュア モビリティ クライアントの修正済み バージョンは計画されません。

脆弱性が存在しない製品

Apple iOS のための Cisco AnyConnect セキュア モビリティ クライアントおよび IPsec だけ Cisco VPN Client はこれらの脆弱性から影響を受けません。

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

細部

Cisco AnyConnect セキュア モビリティ クライアントは Cisco IOSソフトウェアを実行している Cisco 5500 シリーズ 適応型セキュリティ アプライアンス（ASA）およびデバイスへの IPsec（IKEv2）または SSL バーチャル プライベート ネットワーク （VPN）セキュア接続をリモートユーザに与える Cisco NEXT-GENERATION VPN クライアントです。

Cisco AnyConnect セキュア モビリティ クライアントは次の脆弱性から影響を受けます:

任意 プログラムの実行脆弱性

Cisco AnyConnect セキュア モビリティ クライアントは VPN ヘッドエンドからのリモートユーザに展開することができますかまたはエンドポイントは VPN ヘッドエンドに接続する前に、配置前として知られているプロセス インストールすることができます。 Cisco AnyConnect セキュア モビリティ クライアントが前展開されるとき、クライアントソフトウェアは他のアプリケーションのような実行インストールされ。

Cisco AnyConnect セキュア モビリティ クライアントが VPN ヘッドエンドから展開されるとき、VPN ヘッドエンドへの SSL 接続は Webブラウザを使用して開始されます。 ユーザがログオンした後、ブラウザは門脈ウィンドウを表示する、ユーザが「開始する AnyConnect」リンクをクリックするとき、Cisco AnyConnect セキュア モビリティ クライアントのダウンロードのプロセスは開始されます。 この操作により最初ににダウンロードおよび実際の Cisco AnyConnect セキュア モビリティ クライアントを実行することを援助するブラウザをダウンロードします「助手」

アプリケーションを引き起こします。 ヘルパー アプリケーションはブラウザが AcriveX コントロールを利用することができる場合 Linux および MacOS X プラットフォームの Javaアプレット、および Windows プラットフォームの Javaアプレットか ActiveX コントロールです。 ダウンロードされたヘルパー アプリケーションはユーザの Webブラウザの発生サイトという点において実行されます。 ヘルパー アプリケーションは VPN ヘッドエンドからそして Cisco AnyConnect セキュア モビリティ クライアントをダウンロードし、それを実行します。

ヘルパー アプリケーションはきちんとダウンロードされた Cisco AnyConnect セキュア モビリティ クライアント実行可能モジュールの信頼性をクライアントが VPN ヘッドエンドから展開されるとき検証しません。 攻撃者は正常な VPN Web ログイン ページとして考慮された悪意のある Webページを作成し、他の脆弱性の社会工学か不正利用によってそれにアクセスするためにユーザを、誘惑する可能性があります。 これは攻撃者がヘルパー アプリケーションが影響を受けたユーザのマシンでダウンロードし、実行する任意実行可能モジュールを供給することを可能にします。 この任意実行可能モジュールは Webブラウザが動作した同じオペレーティング システム特権と実行されます。

コンポーネントの信頼性を VPN ヘッドエンドから検証する Cisco AnyConnect セキュア モビリティ クライアント 使用コードの署名の修正済み バージョンはダウンロードしました。

この脆弱性は Microsoft ウィンドウ プラットフォームの Cisco AnyConnect セキュア モビリティ クライアントのための Cisco バグ ID CSCsy00904 （登録ユーザのみ）と Linux および Apple MacOS X プラットフォームの Cisco AnyConnect セキュア モビリティ クライアントのための Cisco バグ ID CSCsy05934 （登録ユーザのみ）で文書化されています。 よくある脆弱性および公開（CVE） ID CVE-2011-2039（CSCsy00904 のために）および CVE-2011-2040 はこれらの脆弱性に（CSCsy05934 のために）割り当てられました。

任意 プログラムの実行脆弱性に関する追加問題

Cisco AnyConnect セキュア モビリティ クライアントと提供された VPN ヘッドエンドからダウンロードされるダウンロードされたコンポーネントを検証しないコンポーネントの信頼性を検証するために ActiveX コントロールおよび Javaアプレットの新しい バージョンがコードの署名を利用する間、今でも古いバージョンの問題があることに注目して下さい。 攻撃者は技師 A Webページ ActiveX コントロールまたは Javaアプレットの影響を受けたバージョンを供給し、まだ信頼性 検証の欠如が理由で任意 プログラムの実行を達成するかもしれません。

ActiveX コントロールの古いバージョンのリスクを軽減することは次のように達成することができます:

- 固定 Cisco AnyConnect セキュア モビリティ クライアント バージョンを VPN ヘッドエンドでロードし、VPN 接続を確立して下さい（Webブラウザかスタンドアロン クライアントによって）。 この操作によりインストールします ActiveX コントロールの新しい バージョンを含む Cisco AnyConnect セキュア モビリティ クライアントの新しい バージョンは。 これが発生する場合、ActiveX コントロールの古いバージョンは 1 つがダウンロードのために示され

る場合インスタンス化 されません。
- 前導入 エンタープライズ ソフトウェア アップグレード インフラストラクチャによる Cisco AnyConnect セキュア モビリティ クライアントの修正済み バージョン。 この操作は前の推奨事項と同じ結果を達成します -- それは 1 つがダウンロードのために示される場合古い、制御の脆弱なバージョンがインスタンス化 されないように新しい、ActiveX コントロールの修正済み バージョン展開します。
- VPN ヘッドエンドからのクライアントを展開することが必要ではない場合、Cisco AnyConnect セキュア モビリティ クライアント ActiveX コントロールのためのキル ビットはローカルで設定することができます。 この操作は ActiveX コントロールがあらゆるシナリオの下でインスタンス化 されることを防ぎます。 キル ビットを設定 するための手順はこの文書の範囲を超えてあります; マイクロソフトのサポート技術情報を詳細についてはマイクロソフトのサポート技術情報で参照される http://support.microsoft.com/kb/240797 および Microsoft セキュリティー の 脆弱性リサーチ及び防御の「Kill-bit FAQ」ブログ ポストの Internet Explorer の実行「から」ActiveX コントロールを停止する方法を参照して下さい。 Cisco AnyConnect セキュア モビリティ クライアントが使用する ActiveX コントロールのための CLSID （ クラス識別子 ）は 55963676-2F5E-4BAF-AC28-CF26AA587566 であり、ProgID （ プログラム 識別子 ）は "Cisco.AnyConnect.VPNWeb.1" です。 この CLSID がコードの署名検証を設定する ActiveX コントロールの新しい バージョンと変更しなかったことに注目して下さい。

Javaアプレットの古いバージョンのリスクを軽減することは Java SE 6 アップデート 14 と導入される瓶ブラックリスト機能を使用して、脆弱なバージョン古いブラックリストに載せることによって達成することができます。 瓶ブラックリスト機能の情報に関しては Java SE 6 アップデートを http://www.oracle.com/technetwork/java/javase/6u14-137039.html で利用可能 な 14 のリリース ノート参照して下さい。

ブラックリストに載せられるべき JARファイルは次の SHA-1 メッセージ要約によって識別されます:

```
# 2.3.0254, 2.3.1003, 2.3.2016, 2.4.0202, 2.4.1012,
# 2.5.0217, 2.5.1025, 2.5.2001, 2.5.2006, 2.5.2010,
# 2.5.2011, 2.5.2014, 2.5.2017, 2.5.2018, 2.5.2019
SHA1-Digest-Manifest : x17xGEFzBRXY2pLtXiIbp8J7U9M=

# 2.2.0133, 2.2.0136, 2.2.0140
SHA1-Digest-Manifest : ya6YNTzMCFYUO4lwhmz9OWhhIz8=

# 2.0.0343, 2.1.0148
SHA1-Digest-Manifest : YwuPyF/KMcxcQhgxilzNybFM2+8=
```

ローカル特権 拡大脆弱性

権限のないユーザは LocalSystem アカウントのそれらにログオン（ SBL ）機能の前にによって有効に し、Windows ログオン画面の Cisco AnyConnect セキュア モビリティ クライアント グラフィカル ユーザ インターフェイスとの相互作用特権を開始するを上げることができます。

この問題を防ぐために、Cisco AnyConnect セキュア モビリティ クライアントの修正済み バージョンは Windows ログオン画面で表示するときクライアントのグラフィカル ユーザ インターフェ

イスで可能性のあるである相互対話の量を制限します。

この脆弱性は SBL 機能が Linux および MacOS X クライアントによってサポートされないので Windows のための Cisco AnyConnect セキュア モビリティ クライアントだけ影響を与えます。

この脆弱性は Cisco バグ ID CSCta40556 （登録ユーザのみ）で文書化されています、CVE ID CVE-2011-2041 を割り当てられました。

回避策

このアドバイザリに説明がある脆弱性のための回避策がありません。

固定ソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

脆弱性	プラットフォーム	First Fixed Release（修正された最初のリリース）
任意 プログラムの実行脆弱性	Microsoft Windows	2.3.185
	Linux、Apple Mac OS X	2.5.3041 および 3.0.629
ローカル特権 拡大脆弱性	Microsoft Windows	2.3.254
	Linux、Apple Mac OS X	Not affected

推奨されるリリース

次 の テーブルはすべての推奨されるリリースをリストします。 これらの推奨されるリリースはこのアドバイザリですべての脆弱性のための修正が含まれています。 Cisco はリリースにアップグレードすることを推奨しますこれらの推奨されるリリースよりまたはそれ以降と等しい。

メジャー リリース	推奨リリース
2.5.x	2.5.3046
3.0.x	3.0.1047

ソフトウェアのダウンロード

Cisco AnyConnect セキュア モビリティ クライアントは Cisco.com の Software Center http://www.cisco.com/cisco/software/navigator.html を参照することおよびから製品 > Security > バーチャル プライベート ネットワーク（VPN） > Cisco VPN Client > Cisco AnyConnect セキュア モビリティ クライアントへのによってナビゲート ダウンロードすることができます。

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに説明がある脆弱性の不正利用に気づいていません。 公共エクスプロイト コードは任意 プログラムの実行脆弱性を不正利用するように設計されている Metasploit フレームワーク モジュールの形でリリースされました。

任意 プログラムの実行脆弱性は広い Elazar によって検出され、Cisco に iDefense によって報告されました。 Cisco はこの脆弱性を報告すると脆弱性の調整された公開の方に私達とはたらくことに iDefense に感謝することを望みます。

ローカル特権 拡大脆弱性は顧客によって Cisco に報告されました。

ソース

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110601-ac

改訂履歴

Revision 2.0	2011-July-11	Java SE 6 アップデート 14 およびそれ以降の瓶ブラックリスト機能を使用してブラックリストに載せられるべき瓶の明らかなダイジェストはこのアドバイザリの前のバージョンで不正確でした。 このアップデートは正しいダイジェストを提供します。
リビジョン 1.2	2011-July-07	オリジナル推奨されるリリースが、2.5.3041、Cisco バグ ID CSCtq84525 による cisco.com でもはや利用できないので 2.5.x 推奨されるリリースとして指定 2.5.3046。
リビジョン 1.	2011-June-	任意 プログラムの実行脆弱性のアクセス複雑な状況に関して受け取ったフィードバックを反映する更新済 CVSS スコア。 「不正利用事例と公式発表」セクションを Metasploit フレームワーク モジュールのアベイラビリティを任意 プログラムの実行脆弱性を不正利用するために示すよ

1	06	うにアップデートしました。
リビジョン1.0	2011-June-01	Initial public release.

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。