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

Critical

アドバイザリーID : cisco-sa-20120620-ac

初公開日 : 2012-06-20 16:00

最終更新日 : 2012-10-18 15:31

バージョン 2.1 : Final

CVSSスコア : 9.3

回避策 : No Workarounds available

Cisco バグ ID : CSCtw48681 CSCtz76128 CSCtz78204 CSCty45925 CSCtw47523 CSCtx74235

CVE-2012-2494
CVE-2012-2495
CVE-2012-2496
CVE-2012-4655
CVE-2012-2493

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 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:

- Cisco AnyConnect セキュア モビリティ クライアント VPN Downloader 任意のコード実行脆弱性
- Cisco AnyConnect セキュア モビリティ クライアント VPN Downloader ソフトウェア ダウングレード脆弱性
- Cisco AnyConnect セキュア モビリティ クライアントおよび Cisco Secure Desktop Hostscan Downloader ソフトウェア ダウングレード脆弱性
- Cisco AnyConnect セキュア モビリティ クライアント 64 ビット Java VPN Downloader 任意のコード実行脆弱性
- Cisco Secure Desktop 任意のコード実行脆弱性

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。 これらの脆弱性に対しては回避策があります。 このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac

該当製品

脆弱性のある製品

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
Cisco AnyConnect セキュア モビリティ クライアント VPN Downloader 任意のコード実行脆弱性	Microsoft Windows	• 2.5 MR6 以前の 2.x リリース（2.5.6005）
	Linux、Apple MacOS	• 2.5 MR6 以前の 2.x リリース（2.5.6005） • 3.0 MR8 以前の 3.0.x リリース（3.0.08057）
Cisco AnyConnect セキュア モビリティ クライアント VPN Downloader ソフトウェア ダウングレード脆弱性	Microsoft Windows	• 2.5 MR6 以前の 2.x リリース（2.5.6005） • 3.0 MR8 以前の 3.0.x リリース（3.0.08057）
	Linux、Apple MacOS X	• 2.5 MR6 以前の 2.x リリース（2.5.6005）

		• 3.0 MR8 以前の 3.0.x リリース（3.0.08057）
Cisco AnyConnect セキュア モビリティ クライアントおよび Cisco Secure Desktop Hostscan Downloader ソフトウェア ダウングレード脆弱性	Microsoft Windows	• 3.0 MR8 以前の AnyConnect 3.0.x リリース（3.0.08057） • 3.0MR8 以前の Hostscan 3.0.x リリース（3.0.08062） • 3.6.6020 以前の Cisco Secure Desktop リリース
	Linux、Apple MacOS X	• 3.0 MR8 以前の AnyConnect 3.0.x リリース（3.0.08057） • 3.0MR8 以前の Hostscan 3.0.x リリース（3.0.08062） • 3.6.6020 以前の Cisco Secure Desktop リリース
Cisco AnyConnect セキ	64 ビット	

ュア モビリティ クライアント 64 ビット Java VPN Downloader 任意のコード実行脆弱性	Linux	• 3.0 MR7 以前の 3.0.x リリース（3.0.7059）
Cisco Secure Desktop 任意のコード実行脆弱性	Microsoft ウィンドウ、Linux、Apple Mac OS X	• 3.6.6020 以前の Cisco Secure Desktop リリース

注: Cisco AnyConnect セキュア モビリティ クライアントの Microsoft ウィンドウ モービル バージョンは任意のコード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。

脆弱性を含んでいないことが確認された製品

これらの脆弱性は Apple iOS、Cisco Cius、または Google Android で動作する Cisco AnyConnect クライアントソフトウェアに影響を与えません。 それらのバージョンはこれらの脆弱性が含まれている自己アップデート ダウンロード メカニズムをサポートしません。

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。

詳細

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 2 つの方法で展開することができます: 前展開し、Web 展開して下さい。 前展開シナリオでは、Cisco AnyConnect セキュア モビリティ クライアントはエンドユーザによってまたは可能性のある 企業の配備ツールで従来のデスクトップ ソフトウェアとしてインストールされているか、またはアップグレードされます。 Web 展開シナリオでは、Cisco AnyConnect セキュア モビリティ クライアントはヘッドエンドでインストールされるパッケージによってインストールされているか、またはアップグレードされます。 更に、Web 展開シナリオは 2 つの方法で始めることができます: スタンドアロン開始および WebLaunch 開始。 スタンドアロン開始の間に、エンドユーザ システムによっては AnyConnect クライアントによって配置したパッケージを受け取るためにヘッドエンドが接触します。 WebLaunch 開始の間、Downloader コンポーネントをインスタンス化 する Cisco AnyConnect セキュア モビリティ クライアントをインストールするか、またはアップグレードするために試みがプロンプト表示される Webサイトにアクセスするエンドユーザ システム。 正常な動作では、こ

の Webサイトは clientless ポータルです; 悪意のある不正侵入の間に、ホストしたどの Webサイトでも信頼できるサイトを脆弱なコンポーネントのコピー マスカレードし、ユーザを脆弱なコンポーネントをインスタンス化 するように確信させるように試みる可能性があります。

この状況報告すべてに説明がある脆弱性は WebLaunch 始められた Web 配備を行うのに使用されるソフトウェア アップデート メカニズムで不正利用されます。 エンドユーザ システムにどのようにに関係なく展開されたか Cisco AnyConnect セキュア モビリティ クライアントのすべての影響を受けたバージョンは、不正利用に敏感です。 さらに、WebLaunch コンポーネントが Cisco によって署名し、これらの脆弱性が理由で悪意のある ソフトウェアの任意インストールを可能にすることができるので脆弱な WebLaunch Downloader コンポーネントをインスタンス化 するどのエンドユーザ システムでも決してずっと Cisco AnyConnect セキュア モビリティ クライアントをインストールしていないシステムを含んで、影響を与えられるかもしれません。

固定 Ciscoソフトウェアに欠けるかもしれないシステムはこの脆弱性によって影響を与えることができます。 Cisco は Microsoft および Oracle をソフトウェア アップデート チャネルを通して AcriveX コントロールおよび Javaアプレットをブラックリストに載せるように要求しました。 Microsoft は脆弱な AcriveX コントロールのためのシステム全体の Kill-bit を設定する Windows Security Advisory をリリースしました（ 2736233 ）、Oracle は Java SE 6 （脆弱な署名された Javaアプレットをブラックリストに載せる Java SE 7 （ 9 ）アップデートに更新をおよび アップデート 37 ）リリースし。 署名された Javaアプレットをブラックリストに載せることによって見つけられる機能の変更に関する詳細については「回避策」セクションを参照して下さい。

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

Cisco AnyConnect セキュア モビリティ クライアント VPN Downloader 任意のコード実行脆弱性:

Cisco AnyConnect セキュア モビリティ クライアントは任意のコード実行脆弱性が含まれています。 非認証は、リモート攻撃者 Cisco AnyConnect セキュア モビリティ クライアントのための WebLaunch 機能を実行する ActiveX または Java コンポーネントを受け取ったシステムの任意のコードを実行する可能性があります。 攻撃者はエンドユーザによる実行のための ActiveX または Java 脆弱なコンポーネントを供給するかもしれません。 ActiveX および Java 影響を受けたコンポーネントは十分な入力の検証を行わないし、その結果、攻撃者を影響を受けたシステムに任意のコードを提供することを許可し、ユーザの Webブラウザ セッションの特権のコードを実行するかもしれません。 この脆弱性を不正利用するために、攻撃者はユーザを悪意のある Webページを参照し、脆弱な ActiveX コントロールか Javaアプレットを実行するように確信させる必要があります。 ユーザーのブラウザー設定によっては、制御かアプレットの実行のプロセスは脆弱な AcriveX コントロールおよび Javaアプレットが Cisco によって暗号に署名するのでほとんどユーザー操作を必要とするかもしれません。

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 Downloader プロセスが WebLaunch 開始の間に規定 される任意バイナリの実行をサポートしないようにすることによってこの脆弱性を解決します。

この脆弱性 Cisco バグ ID CSCtw47523 （ 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-2012-2493 は割り当てられました。

Cisco AnyConnect セキュア モビリティ クライアント VPN Downloader ソフトウェア ダウングレード脆弱性:

Cisco AnyConnect セキュア モビリティ クライアントは攻撃者が前ソフトウェア バージョンに Cisco AnyConnect セキュア モビリティ クライアント ソフトウェア バージョンをダウングレードことを可能にする可能性がある脆弱性が含まれています。 非認証により、リモート攻撃者 クライアントソフトウェアのより古いバージョンをダウンロードし、インストールするために Cisco AnyConnect セキュア モビリティ クライアントの影響を受けたバージョンをインストールしたシステムを引き起こす可能性があります。 WebLaunch のために使用する ActiveX および Java 影響を受けたコンポーネントは十分な入力の検証を行わないし、その結果、攻撃者を Cisco によって署名するコードの以前のバージョンを提供することを許可するかもしれません。 Cisco AnyConnect セキュア モビリティ クライアント ソフトウェアのより古いバージョンはシステムの最初のソフトウェア バージョンに含まれなかった、追加脆弱性--にシステムを可能性があります脆弱性がさらす。 この脆弱性を不正利用するために、攻撃者はユーザを悪意のある Webページを参照し、脆弱な ActiveX コントロールか Javaアプレットを実行するように確信させる必要があります。 ユーザーのブラウザー設定によっては、制御かアプレットの実行のプロセスは脆弱な AcriveX コントロールおよび Javaアプレットが Cisco によって暗号に署名するのでほとんどユーザー操作を必要とするかもしれません。

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 WebLaunch 開始の間にダウンロードされるインストール済みソフトウェアのタイムスタンプより古くない署名されたコードのタイムスタンプことの確認によってこの脆弱性を解決します。

この脆弱性 Cisco バグ ID CSCtw48681 （ 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-2012-2494 は割り当てられました。

Cisco AnyConnect セキュア モビリティ クライアントおよび Cisco Secure Desktop Hostscan Downloader ソフトウェアは脆弱性をダウングレード:

Cisco AnyConnect セキュア モビリティ クライアントは攻撃者が前ソフトウェア バージョンに影響を受けたソフトウェアをダウングレードことを可能にする可能性がある脆弱性が含まれています。 この脆弱性は Cisco Secure Desktop にまたあります。 非認証により、リモート攻撃者 クライアントソフトウェアのより古いバージョンをダウンロードし、インストールするために Cisco AnyConnect セキュア モビリティ クライアントまたは Cisco Secure Desktop の影響を受けたバージョンをインストールしたシステムを引き起こす可能性があります。 これらの影響を受けたソフトウェア プログラムの ActiveX および Java 影響を受けたコンポーネントは十分な入力の検証を行わないし、その結果、攻撃者を Cisco によって署名するコードの以前のバージョンを提供することを許可するかもしれません。 従って Cisco AnyConnect セキュア モビリティ クライアント ソフトウェアまたは Cisco Secure Desktop ソフトウェアのより古いバージョンはシステムの

最初のソフトウェア バージョンになかった追加脆弱性--にシステムをさらす脆弱性が、含まれている可能性があります。 この脆弱性を不正利用するために、攻撃者はユーザを悪意のあるWebページを参照し、脆弱な ActiveX コントロールか Javaアプレットを実行するように確信させる必要があります。 ユーザーのブラウザー設定によっては、制御かアプレットの実行のプロセスは脆弱な AcriveX コントロールおよび Javaアプレットが Cisco によって暗号に署名するのでほとんどユーザー操作を必要とするかもしれません。

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 WebLaunch 開始の間にダウンロードされるインストール済みソフトウェアのタイムスタンプより古くない署名されたコードのタイムスタンプことの確認によってこの脆弱性を解決します。

この脆弱性 Cisco バグ ID CSCtx74235 （ 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-2012-2495 は割り当てられました。

Cisco AnyConnect セキュア モビリティ クライアント 64 ビット Java VPN Downloader 任意のコード実行脆弱性:

Cisco AnyConnect セキュア モビリティ クライアントは任意のコード実行脆弱性が含まれています。 非認証は、リモート攻撃者 Cisco AnyConnect セキュア モビリティ クライアントのための WebLaunch VPN Downloader 機能を実行する 64 ビット Javaアプレットを受け取ったシステムの任意のコードを実行する可能性があります。 攻撃者はエンドユーザによる実行のための Java 脆弱なコンポーネントを供給するかもしれません。 Java 影響を受けたコンポーネントは十分な入力の検証を行わないし、その結果攻撃者を任意のコードを影響を受けたシステムに提供し、ユーザの Webブラウザ セッションの特権のコードを実行することを許可する可能性があります。 この脆弱性を不正利用するために、攻撃者はユーザを悪意のある Webページを参照し、脆弱な Javaアプレットを実行するように確信させる必要があります。 影響を受けた Javaアプレットは Cisco によって暗号に署名しません。

この脆弱性から影響を受ける Javaアプレットは Cisco によって署名しないし、サポートされていないコードとして以前に配られました。 このコードはリリース 3.0 MR7 から削除されました（3.0.7059）。

この脆弱性 Cisco バグ ID CSCty45925 （ 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-2012-2496 は割り当てられました。

Cisco Secure Desktop 任意のコード実行脆弱性

Cisco Secure Desktop は任意のコード実行脆弱性が含まれています。 非認証は、リモート攻撃者 Cisco Secure Desktop のための WebLaunch 機能を実行する ActiveX または Java コンポーネントを受け取ったシステムの任意のコードを実行する可能性があります。 攻撃者はエンドユーザによる実行のための ActiveX または Java 脆弱なコンポーネントを供給するかもしれません。 ActiveX および Java 影響を受けたコンポーネントは十分な入力の検証を行わないし、その結果、攻撃者を影響を受けたシステムに任意のコードを提供することを許可し、ユーザの Webブラウザ

セッションの特権のコードを実行するかもしれません。 この脆弱性を不正利用するために、攻撃者はユーザを悪意のある Webページを参照し、脆弱な ActiveX コントロールか Javaアプレットを実行するように確信させる必要があります。 ユーザーのブラウザー設定によっては、制御かアプレットの実行のプロセスは脆弱な AcriveX コントロールおよび Javaアプレットが Cisco によって暗号に署名するのでほとんどユーザー操作を必要とするかもしれません。

Cisco Secure Desktop の修正済み バージョンは Downloader プロセスが WebLaunch 開始の間に規定 される任意バイナリの実行をサポートしないようにすることによってこの脆弱性を解決します。

この脆弱性 Cisco バグ ID CSCtz76128 （ 登録ユーザのみ ）および CSCtz78204 （ 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-2012-4655 は割り当てられました。

Cisco AnyConnect VPN、Cisco Secure Desktop および Cisco Hostscan Downloader 脆弱性に関する追加問題:

Cisco AnyConnect セキュア モビリティ クライアントと出荷する ActiveX コントロールおよび Javaアプレットの新しい バージョンはヘッドエンドからダウンロードされるコンポーネントの信頼性を検証するためにコードの署名を利用します; ただし、より古いバージョンはダウンロードされたコンポーネントを検証しません。 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 コントロールのより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:

- Cisco AnyConnect セキュア モビリティ クライアントの修正済み バージョンをヘッドエンドでロードし、Webブラウザかスタンドアロン クライアントによってアップグレードを開始して下さい。 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。 このインストールが発生する場合、Cisco AnyConnect セキュア モビリティ クライアントはシステムでもはや ActiveX コントロールの割り当てより古いバージョン実行しません。
- 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って Cisco AnyConnect セキュア モビリティ クライアントの修正済み バージョンを前展開して下さい。 この操作は前の推奨事項と同じ結果を達成し、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。 このインストールが発生する場合、Cisco AnyConnect セキュア モビリティ クライアントはシステムでもはや ActiveX コントロールの割り当てより古いバージョン実行しません。
- 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 Kill-bit 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することを防ぎます。 Kill-bit 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。 Kill-bit の設定によって見つけられる機能の変更についての詳細についてはこの文書の「回避策」セクションを参照して下さい。

Cisco AnyConnect セキュア モビリティ クライアントが使用する脆弱な VPN Downloader AcriveX コントロールのための CLSIDs（クラス識別子）はあります（CSCtw47523 および CSCtw48681）:

Cisco AnyConnect VPN バージョン	CLSID
<= 2.5.3046、3.0.0629 - 3.0.2052	55963676-2F5E-4BAF-AC28-CF26AA587566
2.5.3051 - 2.5.3055、3.0.3050 - 3.0.7059	CC679CB8-DC4B-458B-B817-D447B3B6AC31

Cisco AnyConnect セキュア モビリティ クライアントが使用する脆弱な Cisco Secure Desktop および Hostscan AcriveX コントロールのための CLSIDs（クラス識別子）はあります（Cisco Secure Desktop: CSCtz76128 および CSCtz78204 および Hostscan: CSCtx74235）:

Cisco Secure Desktop Hostscan バージョン	Cisco AnyConnect Hostscan バージョン	CLSID
3.1.1.45 - 3.5.841	-	705EC6D4-B138-4079-A307-EF13E4889A82
3.5.1077 - 3.5.2008	3.0.0629 - 3.0.1047	F8FC1530-0608-11DF-2008-0800200C9A66
3.6.181 - 3.6.5005	3.0.2052 - 3.0.7059	E34F52FE-7769-46ce-8F8B-5E8ABAD2E9FC

署名された Javaアプレットの古いバージョンの実行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 JAR ブラックリスト機能を使用して脆弱なバージョンを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。 JAR 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。 この軽減が署名されたアプレットのためだけに関連しているので Cisco 問題 CSCty45925 に説明がある**無署名の Javaアプレットが**ブラックリストに載せることができないことに注目して下さい。 署名された Javaアプレットをブラックリストに載せることによって見つけられる機能の変更についての詳細については「回避策」セクションを参照して下さい。

VPN Downloader 脆弱性から影響を受ける Cisco AnyConnect セキュア モビリティ クライアント JARファイルのための SHA-1 メッセージ要約は（CSCtw47523 および CSCtw48681）次の通りです:

Cisco AnyConnect VPN ソフトウェア バージョン	Java SHA-1 メッセージ要約
2.0.0343 - Windows	L0l3WOuMNWujmXo5+O/GtmGyyYk=
2.0.0343 - Linux	uWffvhFaWVw3lrER/SJH7Hl4yFg=
2.1.0148	YwuPyF/KMcxcQhgxilzNybFM2+8=
2.2.0133 - 2.2.0140	ya6YNTzMCFYUO4lwhmz9OWhhlz8=
2.3.0185 - 2.3.1003	D/TyRle6Sl+CDuBFmdOPy03ERaw=
2.3.2016 - 2.5.2019	x17xGEFzBRXY2pLtXilbp8J7U9M=
2.5.3046 - 2.5.3055	0CUppG7J6lL8xHqPCnA377Koahw=
3.0.0629	nv5+0eBNHpRIsB9D6TmEbWoNCTs=
3.0.1047 - 3.0.5080	qMVUh9i3yJcTKpuZYSFZH9dspqE=

Cisco Secure Desktop および Hostscan 脆弱性（Cisco Secure Desktop から影響を受ける Cisco AnyConnect セキュア モビリティ クライアントおよび Cisco Secure Desktop JARファイルのための SHA-1 メッセージ要約: CSCtz76128 および CSCtz78204 および Hostscan: CSCtx74235 は）次の通りです:

Cisco	Cisco	Java SHA-1 メッセージ要約

Secure Desktop Hostscan バージョン	AnyConnect Hostscan バージョン	
3.1.1.45	-	3aJU1qSK6lYmt5MSh2IIlj5G1XE=
3.2.0.136	-	l93uYyDZGyynzYTknp31yyuNivU=
3.2.1.103	-	eJfWm86yHp2Oz5U8WrMKbpv6GGA=
3.2.1.126	-	Q9HXbUcSCjhwkgpk5NNVG/sArVA=
3.3.0.118	-	cO2ccW2cckTvpR0HVgQa362PyHI=
3.3.0.151	-	cDXEH+bR01R8QVxL+KFKYqFgsR0=
3.4.373	-	lbhLWSopUlqPQ08UVIA927Y7jZQ=
3.4.1108	-	vSd+kv1p+3jrVK9FjDCBJcoy5us=
3.4.2048	-	TFYT30lirbYk89l/uKykM6g2cVQ=
3.5.841	-	Y82nn7CFTu1XAOCDjemWwyPLssg=
3.5.1077	-	PVAkXuUCgiDQI19GPrw01Vz4rGQ=
3.5.2001	-	C4mtepHAyIKiAjjqOm6xYMo8TkM=
3.5.2003	-	l4meuozuSFLkTZTS6xW3sixdlBI=
3.5.2008	-	B1NaDg834Bgg+VE9Ca+tDZOd2BI=
3.6.181	-	odqJCMnKdgvQLOCAMSWEj1EPQTc=
3.6.185	-	WyqHV02O4PYZkcbidH4HKlp/8hY=
3.6.1001	-	HSPXCvBNG/PaSXg8thDGqSeZlR8=
-	3.0.0629 - 3.0.1047	OfQZHjo8GK14bHD4z4dDIp4ZFjE=
-	3.0.2052	8F4F0TXA4ureZbfEXWIFm76QGg4=
-	3.0.3054 - 3.0.4016	bOoQga+XxC3j0HiP552+fYCdswo=
-	3.0.4216 - 3.0.4235	WX77FlRyFyeUriu+xi/PE1uLALU=

3.6.2002	3.0.5009	g3mA5HqcRBIKaUVQsapnKhOSEas=
3.6.3002	-	trhKo6XiSGxRrS//rCL9e3Ca6D4=
3.6.4021	3.0.5075 - 3.0.5080	obWCTaz3uOZwDBDZUsbrrTKoDig=
3.6.5005	3.0.7042 - 3.0.7059	iMHjGyv5gEnTi8uj68yzalml8XQ=

回避策

ブラックリストは手動で、によって" Details "セクションで、または Microsoft から更新を加えること提供される手順に基づいて実施することができます（ 2736233 ）または Oracle （ Java SE 6 アップデート 37 および ActiveX CLSIDs か Javaアプレット メッセージ要約が含まれている 9 ） Java SE 7 アップデート。 脆弱な ActiveX コントロール CLSIDs のブラックリストおよび Javaアプレット メッセージ要約を実施することを選択するだれでも脆弱なコードがインスタンス化 することを防ぐことができます。 その結果、脆弱なソフトウェアインストーレーションの WebLaunch 開始およびアップグレードは防がれます; ただし、修正済みソフトウェアの WebLaunch スタンドアロン方式および開始によって始められた前展開されたソフトウェアは機能し続けます。

注: 暗号に署名された制御またはアプレットの脆弱性の何れかのために、Cisco AnyConnect セキュア モビリティ クライアントがシステムで決してインストールされていなくても信頼するどのシステムでも Cisco 署名証明書 チェーン影響を与えられるかもしれません。 ActiveX コントロールを使用する Kill-bit および Java メッセージ要約 回避策は Cisco AnyConnect セキュア モビリティ クライアントがない保護しましたりまたはインストールされないことをシステムを。

ネットワークの on Cisco 配置されたデバイスの場合もある軽減はこの状況報告に Cisco によって加えられる知性ドキュメントガイドで利用できます: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20120620-ac

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性と完全なアップグレード ソリューション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。

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)

Cisco AnyConnect セキュア モビリティ クライアント VPN Downloader 任意のコード実行脆弱性	Microsoft Windows	2.5 MR6（2.5.6005）
	Linux、Apple Mac OS X	2.5 MR6*（2.5.6005）、3.0 MR8（3.0.08057）
Cisco AnyConnect セキュア モビリティ クライアント VPN Downloader ソフトウェア ダウングレード脆弱性	Microsoft Windows	2.5 MR6（2.5.6005）、3.0 MR8（3.0.08057）
	Linux、Apple Mac OS X	2.5 MR6*（2.5.6005）、3.0 MR8（3.0.08057）
Cisco AnyConnect セキュア モビリティ クライアントおよび Cisco Secure Desktop Hostscan Downloader ソフトウェア ダウングレード脆弱性	Microsoft Windows	• AnyConnect 3.0 MR8（3.0.08057） • Hostscan 3.0 MR8（3.0.08062） • Cisco Secure Desktop 3.6.6020
	Linux、Apple Mac OS X	• AnyConnect 3.0 MR8（3.0.08057） • Hostscan 3.0 MR8（3.0.08062） • Cisco Secure Desktop 3.6.6020
Cisco AnyConnect セキュア モビリティ クライアント 64 ビット Java VPN Downloader 任意のコード実行脆弱性	Microsoft Windows	Not affected
	64 ビット Linux	3.0 MR7（3.0.7059）
Cisco Secure Desktop 任意のコード実行脆弱性	Microsoft ウィンドウ、Linux、Apple Mac OS X	Cisco Secure Desktop 3.6.6020

*注： この状況報告で VPN Downloader 脆弱性のための修正が含まれている Mac OS X のための Cisco AnyConnect セキュア モビリティ クライアント 2.5 MR6 はもはや OS X 10.4 をサポートしません。

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状況報告ですべての脆弱性のための修正が含まれています。 Cisco は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リリースにアップグレードすることを推奨します。

ソフトウェア名	メジャーリリース	推奨リリース
Cisco AnyConnect セキュア モビリティ クライアント	2.5.x	2.5 MR6（2.5.6005）
Cisco AnyConnect セキュア モビリティ クライアント	3.0.x	3.0 MR8（3.0.08057）
Hostscan	3.0.x	3.0 MR8（3.0.08062）
Cisco Secure Desktop	3.x	3.6.6020

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やその公表を確認していません。

問題 CSCtw47523 および CSCtw48681 で文書化されています脆弱性は gwslabs.com によって検出され、Cisco に HP のゼロの日コントロールによって報告されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac

改訂履歴

Revision 2.1	2012-October-18	固定 Ciscoソフトウェアの配備を必要としないで WebLaunch 脆弱な制御を無効に する Oracle Java SE 6u37 および Java SE 7u9 の含まれた詳細。
Revision 2.0	2012-September-19	修正はまた Cisco Secure Desktop の脆弱性に対処することリストしなかった CVE-2012-4655 によって記述されているオリジナル状況報告の不注意な省略を、訂正しました。
リビジョン 1.3	2012-September-09	固定 Ciscoソフトウェアの配備を必要としないで WebLaunch 脆弱な制御を無効に する Oracle および Microsoft からの詳しい今後のアップデート。
リビジョ	2012-July-18	Linuxバージョン 2.0.0343 のためのブラックリスト表に Java 追加ハッシュを追

ン 1.2		加しました。
リビジョン 1.1	2012-July-06	メンテナンスリリース (MR) 数の隣のビルド 番号が含まれていることによる明白にされたバージョン。
リビジョン 1.0	2012-June-20	初回公開リリース

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。