Cisco AnyConnectセキュアモビリティクライアントの複数の脆弱性

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、次の脆弱性の影響を受けます。

- Cisco AnyConnectセキュアモビリティクライアントVPNダウンローダにおける任意のコードが実行される脆弱性
- Cisco AnyConnectセキュアモビリティクライアントのVPNダウンローダにおける、ソフトウェアのダウングレードが行われる脆弱性
- Cisco AnyConnectセキュアモビリティクライアントおよびCisco Secure Desktopホストスキャンダウンローダソフトウェアのダウングレードの脆弱性
- Cisco AnyConnectセキュアモビリティクライアントの64ビットJava VPNダウンローダにおける、任意のコードが実行される脆弱性
- Cisco Secure Desktopにおける任意のコード実行の脆弱性

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リリースしています。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。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac

該当製品

脆弱性のある製品

このドキュメントで説明されている脆弱性は、Cisco AnyConnectセキュアモビリティクライアントに適用されます。該当するバージョンは次のとおりです。

脆弱性	Platform	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ダウンローダにおける任意のコードが実行される脆弱性	Microsoft Windows	• 2.5 MR6(2.5.6005)より前の2.xリリース
	Linux、Apple MacOS	• 2.5 MR6(2.5.6005)より前の2.xリリース • 3.0 MR8(3.0.08057)より前の3.0.xリリース
Cisco AnyConnectセキュアモビリティクライアントのVPNダウンローダにおける、ソフトウェアのダウングレードが行われる脆弱性	Microsoft Windows	• 2.5 MR6(2.5.6005)より前の2.xリリース • 3.0 MR8(3.0.08057)より前の3.0.xリリース
	Linux、Apple MacOS X	• 2.5 MR6(2.5.6005)より前の2.xリリース • 3.0 MR8(3.0.08057)より前の3.0.xリリース
Cisco AnyConnectセキュアモビリティクライアントおよびCisco Secure Desktopホストスキャンダ	Microsoft Windows	• 3.0 MR8(3.0.08057)より前のAnyConnect 3.0.xリリース • 3.0MR8(3.0.08062)より前のホストスキャ

ウンローダソフトウェアのダウングレードの脆弱性		ン3.0.xリリース • 3.6.6020よりも前のCisco Secure Desktopリリース
	Linux、Apple MacOS X	• 3.0 MR8(3.0.08057)より前のAnyConnect 3.0.xリリース • 3.0MR8(3.0.08062)より前のホストスキャン3.0.xリリース • 3.6.6020よりも前のCisco Secure Desktopリリース
Cisco AnyConnectセキュアモビリティクライアントの64ビットJava VPNダウンローダにおける、任意のコードが実行される脆弱性	Linux 64ビット	• 3.0 MR7(3.0.7059)より前の3.0.xリリース
Cisco Secure Desktopにおける任意のコード実行の脆弱性	Microsoft Windows、Linux、Apple Mac OS X	• 3.6.6020よりも前のCisco Secure Desktopリリース

注：Microsoft Windows MobileバージョンのCisco AnyConnectセキュアモビリティクライアントは、任意のコードが実行される脆弱性の影響を受けます。Windows Mobile向け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ていません。

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で稼働するCisco AnyConnectクライアントソフトウェアには影響しません。これらのバージョンでは、これら

の脆弱性が含まれている自己更新ダウンロードメカニズムはサポートされていません。

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シスコの次世代VPNクライアントで、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Cisco IOSソフトウェアを実行しているデバイスに対して、リモートユーザにセキュアIPsec(IKEv2)またはSSL仮想プライベートネットワーク(VPN)接続を提供します。

Cisco AnyConnectセキュアモビリティクライアントは、導入前とWeb導入の2つの方法で導入できます。導入前のシナリオでは、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、または企業の導入ツールを介して、従来のデスクトップソフトウェアとしてインストール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、ヘッドエンドにインストールされたパッケージを介してインストールまたはアップグレードされます。さらに、Web導入シナリオは、スタンドアロンの開始とWebLaunchの開始の2つの方法で開始できます。スタンドアロンの開始時に、エンドユーザシステムはAnyConnectクライアントを介してヘッドエンドに接続し、展開されたパッケージを受信します。WebLaunchの開始時に、ダウンローダコンポーネントをインスタンス化しようとするWebサイトにアクセスするエンドユーザシステムは、Cisco AnyConnectセキュアモビリティクライアントをインストールまたはアップグレードするように求められます。通常の運用では、このWebサイトはクライアントレスポータルになります。悪意のある攻撃の際には、脆弱なコンポーネントのコピーをホストしていたWebサイトが信頼できるサイトになりすまして、脆弱なコンポーネントのインスタンスを作成するようユーザを誘導する可能性があります。

このアドバイザリに記載されている脆弱性はすべて、WebLaunchが開始するWeb展開の実行に使用されるソフトウェア更新メカニズムによって不正利用されます。影響を受けるCisco AnyConnectセキュアモビリティクライアントのバージョンはすべて、エンドユーザのシステムにどのように導入されたかに関係なく、不正利用される可能性があります。さらに、WebLaunchコンポーネントはシスコによって署名されているため、これらの脆弱性により悪意のあるソフトウェアが任意にインストールされる可能性があり、WebLaunchダウンローダコンポーネントをインスタンス化するエンドユーザシステムは、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たことがないシステムも含めて、影響を受ける可能性があります。

修正済みのシスコソフトウェアがインストールされていないシステムは、この脆弱性の影響を受ける可能性があります。シスコはMicrosoftとOracleに対し、ソフトウェアアップデートチャネルを通じてActiveXコントロールとJavaアプレットをブラックリストに載せるよう要請しています。Microsoftは、脆弱なActiveXコントロールに対してシステム全体のキルビットを設定するWindowsセキュリティアドバイザリ(2736233)をリリースしました。またOracleは、脆弱な署名付きJavaアプレットをブラックリストに登録するJava SE 6(Update 37)およびJava SE 7(Update 9)のアップデートをリリースしました。署名付きJavaアプレットのブラックリスト登録による機能変更の詳細については、「回避策」セクションを参照してください。

Cisco AnyConnectセキュアモビリティクライアントは、次の脆弱性の影響を受けます。

Cisco AnyConnectセキュアモビリティクライアントVPNダウンローダにおける任意のコードが実行される脆弱性：

Cisco AnyConnectセキュアモビリティクライアントには、任意のコードが実行される脆弱性が存在します。認証されていないリモートの攻撃者が、Cisco AnyConnectセキュアモビリティクライアントのWebLaunch機能を実行するActiveXまたはJavaコンポーネントを受信したシステムで、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に、脆弱なActiveXまたはJavaコンポーネントを提供する可能性があります。該当するActiveXおよびJavaのコンポーネントは十分な入力検証を行わず、その結果、攻撃者が該当システムに任意のコードを配信し、ユーザのWebブラウザセッションの権限で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、攻撃者が悪意のあるWebページにアクセスし、脆弱なActiveXコントロールまたはJavaアプレットを実行するようにユーザを誘導する必要があります。脆弱なActiveXコントロールおよびJavaアプレットはシスコによって暗号署名されているため、ユーザのブラウザの設定によっては、コントロールまたはアプレットを実行するプロセスにユーザの操作はほとんど必要ない場合があります。

修正済みバージョンのCisco AnyConnectセキュアモビリティクライアントは、ダウンローダプロセスがWebLaunchの開始中に指定された任意のバイナリの実行をサポートしないことを保証することで、この脆弱性を修正します。

この脆弱性は、Cisco Bug ID CSCtw47523(登録ユーザ専用)として文書化され、Common Vulnerability and Exposure(CVE)IDとしてCVE-2012-2493が割り当てられています。

Cisco AnyConnectセキュアモビリティクライアントのVPNダウンローダにおける、ソフトウェアのダウングレードに関する脆弱性：

Cisco AnyConnectセキュアモビリティクライアントには、攻撃者がCisco AnyConnectセキュアモビリティクライアントのソフトウェアバージョンを以前のソフトウェアバージョンにダウングレードできる可能性のある脆弱性が存在します。認証されていないリモートの攻撃者が、該当するバージョンの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たシステムに、古いバージョンのクライアントソフトウェアをダウンロードさせ、インストールさせる可能性があります。WebLaunchで使用される該当のActiveXおよびJavaコンポーネントは十分な入力検証を行わず、その結果、攻撃者がシスコによって署名された以前のバージョンのコードを配信する可能性があります。古いバージョンのCisco AnyConnectセキュアモビリティクライアントソフトウェアには、システムの初期ソフトウェアバージョンには存在しなかった脆弱性が含まれており、システムが更なる脆弱性にさらされ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、攻撃者が悪意のあるWebページにアクセスし、脆弱なActiveXコントロールまたはJavaアプレットを実行するようにユーザを誘導する必要があります。脆弱なActiveXコントロールおよびJavaアプレットはシスコによって暗号署名されているため、ユーザのブラウザの設定によっては、コントロールまたはアプレットを実行するプロセスにユーザの操作はほとんど必要ない場合が

あります。

修正済みバージョンのCisco AnyConnectセキュアモビリティクライアントでは、WebLaunchの開始時にダウンロードされる署名済みコードのタイムスタンプがインストール済みソフトウェアのタイムスタンプよりも古くならないように、この脆弱性が修正されています。

この脆弱性は、Cisco Bug ID CSCtw48681(登録ユーザ専用)として文書化され、Common Vulnerability and Exposure(CVE)IDとしてCVE-2012-2494が割り当てられています。

Cisco AnyConnectセキュアモビリティクライアントおよびCisco Secure Desktop Hostscanダウンローダソフトウェアのダウングレードにおける脆弱性：

Cisco AnyConnectセキュアモビリティクライアントには、攻撃者が該当ソフトウェアを以前のソフトウェアバージョンにダウングレードできる可能性のある脆弱性が存在します。この脆弱性は、Cisco Secure Desktopにも存在します。認証されていないリモートの攻撃者が、該当するバージョンのCisco AnyConnectセキュアモビリティクライアントまたはCisco Secure Desktopをインストールしたシステムに、古いバージョンのクライアントソフトウェアをダウンロードさせてインストールさせる可能性があります。該当するソフトウェアプログラムの該当するActiveXおよびJavaコンポーネントでは、十分な入力検証が行われないため、攻撃者によってシスコが署名した以前のバージョンのコードが配信される可能性があります。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ソフトウェアの古いバージョンには、システムの初期ソフトウェアバージョンには存在しなかった脆弱性が含まれている可能性があり、その結果、システムがさらに脆弱性にさらされ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、攻撃者が悪意のあるWebページにアクセスし、脆弱なActiveXコントロールまたはJavaアプレットを実行するようにユーザを誘導する必要があります。脆弱なActiveXコントロールおよびJavaアプレットはシスコによって暗号署名されているため、ユーザのブラウザの設定によっては、コントロールまたはアプレットを実行するプロセスにユーザの操作はほとんど必要ない場合があります。

修正済みバージョンのCisco AnyConnectセキュアモビリティクライアントでは、WebLaunchの開始時にダウンロードされる署名済みコードのタイムスタンプがインストール済みソフトウェアのタイムスタンプよりも古くならないように、この脆弱性が修正されています。

この脆弱性は、Cisco Bug ID CSCtx74235(登録ユーザ専用)として文書化され、Common Vulnerability and Exposure(CVE)IDとしてCVE-2012-2495が割り当てられています。

Cisco AnyConnectセキュアモビリティクライアント64ビットJava VPNダウンローダにおける、任意のコードが実行される脆弱性：

Cisco AnyConnectセキュアモビリティクライアントには、任意のコードが実行される脆弱性が存在します。Cisco AnyConnectセキュアモビリティクライアントのWebLaunch VPNダウンローダ機能を実行する64ビットJavaアプレットを受信したシステムでは、認証されていないリモートの攻撃者が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

に、脆弱なJavaコンポーネントを提供する可能性があります。該当するJavaコンポーネントでは十分な入力検証が行われないため、攻撃者が該当システムに任意のコードを配信し、ユーザのWebブラウザセッションの権限で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、攻撃者が悪意のあるWebページにアクセスして脆弱なJavaアプレットを実行するようにユーザを誘導する必要があります。該当するJavaアプレットには、シスコによる暗号化署名が行われていません。

この脆弱性の影響を受けるJavaアプレットはシスコによって署名されておらず、以前はサポート対象外のコードとして配布されていました。このコードは、リリース3.0 MR7(3.0.7059)から削除されています。

この脆弱性は、Cisco Bug ID CSCty45925(登録ユーザ専用)として文書化され、Common Vulnerability and Exposure(CVE)IDとしてCVE-2012-2496が割り当てられています。

Cisco Secure Desktopにおける任意のコード実行の脆弱性

Cisco Secure Desktopには、任意のコードが実行される脆弱性が存在します。Cisco Secure DesktopのWebLaunch機能を実行するActiveXまたはJavaコンポーネントを受信したシステムでは、認証されていないリモートの攻撃者によって任意のコードが実行され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に、脆弱なActiveXまたはJavaコンポーネントを提供する可能性があります。該当するActiveXおよびJavaのコンポーネントは十分な入力検証を行わず、その結果、攻撃者が該当システムに任意のコードを配信し、ユーザのWebブラウザセッションの権限で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、攻撃者が悪意のあるWebページにアクセスし、脆弱なActiveXコントロールまたはJavaアプレットを実行するようにユーザを誘導する必要があります。脆弱なActiveXコントロールおよびJavaアプレットはシスコによって暗号署名されているため、ユーザのブラウザの設定によっては、コントロールまたはアプレットを実行するプロセスにユーザの操作はほとんど必要ない場合があります。

修正済みバージョンのCisco Secure Desktopでは、WebLaunchの開始時に指定された任意のバイナリの実行がダウンローダプロセスでサポートされないようにして、この脆弱性が修正されています。

この脆弱性は、Cisco Bug ID CSCtz76128(登録ユーザ専用)および CSCtz78204(登録ユーザ専用)として文書化され、Common Vulnerability and Exposure(CVE)IDとしてCVE-2012-4655が割り当てられています。

Cisco AnyConnect VPN、Cisco Secure Desktop、およびCisco Hostscan Downloaderの脆弱性に関するその他の考慮事項：

Cisco AnyConnectセキュアモビリティクライアントに付属する新しいバージョンのActiveXコントロールおよびJavaアプレットでは、コード署名を使用して、ヘッドエンドからダウンロードされたコンポーネントの信頼性を検証します。ただし、古いバージョンでは、ダウンロードされたコンポーネントは検証されません。攻撃者は、ActiveXコントロールまたはJavaアプレットの影響

を受けるバージョンを提供するWebページをエンジニアリングし、真正性検証が行われないために任意のプログラム実行を達成する可能性があります。

古いバージョンのActiveXコントロールのリスクを軽減するには、次の方法があります。

- 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にロードし、Webブラウザまたはスタンドアロンクライアントを使用してアップグレードを開始します。この操作により、新しいバージョンのActiveXコントロールを含む新しいバージョンのCisco AnyConnectセキュアモビリティクライアントがインストールされます。このインストールが発生すると、Cisco AnyConnectセキュアモビリティクライアントは、古いバージョンのActiveXコントロールのシステム上での実行を許可しなくなります。
- 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を通じて、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事前導入します。このアクションは、前の推奨事項と同じ結果を達成し、ActiveXコントロールの新しい修正済みバージョンを導入します。このインストールが発生すると、Cisco AnyConnectセキュアモビリティクライアントは、古いバージョンのActiveXコントロールのシステム上での実行を許可しなくなります。
- ヘッドエンドからクライアントを展開する必要がない場合は、Cisco AnyConnectセキュアモビリティクライアントのActiveXコントロールのキルビットをローカルに設定できます。この操作により、ActiveXコントロールは任意のシナリオでインスタンス化されなくなります。キルビットを設定する手順については、このドキュメントでは説明しません。詳細については、Microsoftサポートの記事「Internet ExplorerでActiveXコントロールの実行を停止する方法」(http://support.microsoft.com/kb/240797)と、Microsoftサポートの記事で参照できるMicrosoft Security Vulnerability Research & Defenseのブログ記事「Kill-Bit FAQ」を参照してください。キルビットの設定によって発生する機能変更の詳細については、このドキュメントの「回避策」セクションを参照してください。

Cisco AnyConnectセキュアモビリティクライアントで使用される脆弱なVPNダウンローダActiveXコントロールのCLSID（クラスID）は次のとおりです(CSCtw47523およびCSCtw48681)。

Cisco AnyConnect VPNのバージョン	CLSID(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、脆弱性のあるCisco Secure DesktopおよびHostscan ActiveXコントロールのCLSID（クラス識別子）は次のとおりです(Cisco Secure Desktop:CSCtz76128およびCSCtz78204、Hostscan:CSCtx74235)。

Cisco Secure Desktopホストスキャンバージョン	Cisco AnyConnectホストスキャンバージョン	CLSID(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

Java SE 6 Update 14で導入されたJARブラックリスト機能を使用して脆弱性のあるバージョンをブラックリストに登録すると、署名付きJavaアプレットの古いバージョンを実行するリスクを軽減できます。JARブラックリスト機能の詳細については、http://www.oracle.com/technetwork/java/javase/6u14-137039.htmlで入手できる『Java SE 6 Update 14』リリースノートを参照してください。この緩和策は署名付きアプレットに対してのみ有効であるため、シスコの不具合CSCty45925で説明されている署名なしJavaアプレットはブラックリストに登録できないことに注意してください。署名付きJavaアプレットのブラックリスト登録による機能変更の詳細については、「回避策」セクションを参照してください。

VPNダウンローダの脆弱性(CSCtw47523およびCSCtw48681)の影響を受けるCisco AnyConnectセキュアモビリティクライアントJARファイルのSHA-1メッセージダイジェストは、次のとおりです。

Cisco AnyConnect VPNソフトウェアのバージョン	Java SHA-1メッセージダイジェスト
2.0.0343:Windows	L0l3WOuMNWWujmXo5+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	x17xGEFzBRXY2pLtXiIbp8J7U9M=
2.5.3046 ~ 2.5.3055	0CUppG7J6IL8xHqPCnA377Koahw=
3.0.0629	nv5+0eBNHpRIsB9D6TmEbWoNCTs=
3.0.1047 ~ 3.0.5080	qMVUh9i3yJcTKpuZYSFZH9dspqE=

Cisco Secure DesktopおよびHostscanの脆弱性の影響を受ける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(Cisco Secure Desktop:CSCtz76128およびCSCtz78204、Hostscan:CSCtx74235)のSHA-1メッセージダイジェストは次のとおりです。

Cisco Secure Desktopホストスキャンバージョン	Cisco AnyConnectホストスキャンバージョン	Java SHA-1メッセージダイジェスト
3.1.1.45	-	3aJU1qSK6IYmt5MSh2IIlj5G1XE=
3.2.0.136	-	l93uYyDZGynzYTknp31yuNivU=
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	-	lbhLWSopUIqPQ08UVIA927Y7jZQ=
3.4.1108	-	vSd+kv1p+3jrVK9FjDCBJcoy5us=
3.4.2048	-	TFYT30IirbYk89l/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/PaSXg8thDGqSeZIR8=
-	3.0.0629 ~ 3.0.1047	/ QZHjo8GK14bHD4z4dDIp4ZFjE=
-	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	g3mA5HqcRBlKaUVQsapnKhOSEas=
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、「詳細」セクションで提供される手順に基づいて、またはActiveX CLSIDまたはJavaアプレットメッセージダイジェストを含むMicrosoft(2736233)またはOracle(Java SE 6 Update 37および Java SE 7 Update 9)のアップデートを適用することによって、手動で適用できます。脆弱なActiveXコントロールCLSIDおよびJavaアプレットメッセージダイジェストのブラックリストを適用することを選択すると、脆弱なコードのインスタンス化を防止できます。その結果、WebLaunchによる脆弱なソフトウェアのインストールとアップグレードの開始は防止されますが、スタンドアロン方式で開始される事前展開済みソフトウェアと、修正済みソフトウェアのWebLaunchによる開始は引き続き機能します。

注：暗号署名付きコントロールまたはアプレットの脆弱性に対しては、Cisco AnyConnectセキュアモビリティクライアントがシステムにインストールされていない場合でも、Ciscoの署名証明書チェーンを信頼するシステムが影響を受ける可能性があります。ActiveXコントロールのキルビットおよびJava Message Digest(JMD)の回避策を使用すると、Cisco AnyConnectセキュアモビリティクライアントがインストールされていない、またはインストールされないシステムが保護されます。

ネットワーク内のシスコデバイスに適用可能な対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。
https://sec.cloudapps.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	Platform	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ダウンローダにおける任意のコードが実行される脆弱性	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のVPNダウンローダにおける、ソフトウェアのダウングレードが行われる脆弱性	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	Microsoft Windows	• AnyConnect 3.0 MR8(3.0.08057)

イアントおよびCisco Secure Desktopホストスキャンダウンローダソフトウェアのダウングレードの脆弱性		• ホストスキャン3.0 MR8 (3.0.08062) • Cisco Secure Desktop 3.6.6020
	Linux、Apple Mac OS X	• AnyConnect 3.0 MR8(3.0.08057) • ホストスキャン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の64ビットJava VPNダウンローダにおける、任意のコードが実行される脆弱性	Microsoft Windows	Not affected
	Linux 64ビット	3.0 MR7 (3.0.7059)
Cisco Secure Desktopにおける任意のコード実行の脆弱性	Microsoft Windows、Linux、Apple Mac OS X	Cisco Secure Desktop 3.6.6020

*注：このアドバイザリで説明されているVPNダウンローダの脆弱性に対する修正が含まれているCisco AnyConnectセキュアモビリティクライアント2.5 MR6 for Mac OS Xは、OS X 10.4をサポートしません。

推奨リリース

次の表に、推奨リリースをすべて示します。これらの推奨リリースには、このアドバイザリに記載されているすべての脆弱性に対する修正が含まれています。シスコでは、これらの推奨リリース、またはそれ以降の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)
ホストスキャン	3.0.x	3.0 MR8(3.0.08062)
Cisco Secure Desktop	3.x	3.6.6020

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

不具合CSCtw47523とCSCtw48681に記載されている脆弱性は、gwslabs.comによって発見され、HPのZero Day Initiativeからシスコに報告されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac

改訂履歴

Revision 2.1	2012年10月18日	Oracle Java SE 6u37およびJava SE 7u9に関する詳細を含む。修正済みのシスコソフトウェアの導入を必要とせずに、脆弱性のあるWebLaunchコントロールを無効にする。
Revision 2.0	2012年9月19日	CVE-2012-4655で記述されているCisco Secure Desktopの脆弱性に対

		する修正も含まれていなかった、元のアドバイザリの不注意による欠落を修正。
リビジョン 1.3	2012年9月9日	MicrosoftとOracleによる今後の詳細なアップデート。修正済みのシスコソフトウェアを導入しなくても、脆弱性のあるWebLaunchコントロールを無効にできる。
リビジョン 1.2	2012年7月18日	Linuxバージョン2.0.0343のブラックリストテーブルにJavaハッシュを追加。
リビジョン 1.1	2012年7月6日	メンテナンスリリース(MR)番号の横にビルド番号を表示することで、バージョンを明確にしました。
リビジョン 1.0	2012年6月20日	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。

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。