Cisco Security Advisory: Cisco ASA 5500 Series Adaptive Security Appliance Clientless VPN ActiveX Control Remote Code Execution Vulnerability

Advisory ID: cisco-sa-20120314-asaclient

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asaclient

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。

Revision 1.1

Last Updated 2012 May 15 14:43 UTC (GMT)

For Public Release 2012 March 14 16:00 UTC (GMT)

目次

要約

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（Cisco ASA）によって配備されているシスコ クライントレス VPN ソリューションは、クライアント システムで ActiveX コントロールを使用してポート転送操作を実行します。Internet Explorer を実行、または Microsoft ActiveX テクノロジーをサポートする別のブラウザを実行している Microsoft Windows ベースのシステムは、シスコ クライントレス VPN ソリューションが稼働しているデバイスに接続された場合、影響を受ける可能性があります。リモートの認証されていない攻撃者がこの問題を不正利用し、悪意のある Web ページにユーザを誘導して接続させ、Web ブラウザの権限によって該当マシンにおいて任意のコードを実行する可能性があります。

影響を受ける ActiveX コントロールは、Cisco ASA によってエンドポイント システムに配布されます。ただし、この脆弱性の不正利用に成功した場合の影響はエンドポイントのシステムに対してのみであり、Cisco ASA デバイスには影響を与えません。

シスコはこの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ました。

こ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、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asaclient

該当製品

シスコ クライントレス VPN は、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスで提供されている機能です。

脆弱性が存在する製品

次のバージョンのいずれかを実行している Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、影響を受ける ActiveX コンポーネントを含んでいます。

Affected Version	Affected Release
Cisco Adaptive Security Appliance Software 7.x	7.1 7.2
Cisco Adaptive Security Appliance Software 8.x	8.0 8.1 8.2 8.3 8.4 8.6

注： Cisco ASA ソフトウェア バージョン 7.0 および 7.1 はソフトウェア メンテナンスが終了しています。Cisco ASA ソフトウェア バージョン 7.0 または 7.1 をご利用のお客様は、サポートされている Cisco ASA ソフトウェア バージョンへのアップグレードに関してシスコ サポート チームにお問い合わせください。

注：シスコ クライントレス VPN ソリューションの該当する実装は、Cisco ASA ソフトウェア バージョン 7.1 のリリースで導入されました。この問題は Cisco PIX ソフトウェアを実行しているデバイスには影響しません。

シスコ クライントレス VPN ソリューションがデバイスで有効にされているかどうかについては、 **show running-config webvpn** コマンドを使用して確認することができます。次の例は、シスコ クライントレス VPN ソリューションが有効にされていることを示しています。

```
ciscoasa# show running-config webvpn
webvpn
 enable outside
```

Microsoft Windows が稼働しているエンド ユーザ システムは、該当するデバイスで、ActiveX テ

クノロジーをサポートしているブラウザからシスコ クライントレス VPN 機能を使用した場合に影響を受ける可能性があります。クラス ID（CLSID）**{B8E73359-3422-4384-8D27-4EA1B4C01232}** で登録された ***cscopf.ocx*** ActiveX コントロールを含むデバイスが影響を受けます。影響を受けるコントロールは Safe for Scripting（SFS）および Safe for Initialization（SFI）の両方がマーク付けされ、影響を受けるコントロールを登録しキャッシュした場合、別の攻撃にさらされる可能性があります。

脆弱性が存在しない製品

- Cisco Firewall Service Module は、この脆弱性の影響を受けません
- Cisco Adaptive Security Appliance Services Module は、この脆弱性の影響を受けません
- シスコ クライントレス VPN ソリューション（WebVPN）を使用する Cisco IOS ソフトウェアベースのデバイスは、この脆弱性の影響を受けません

この脆弱性に該当するその他のシスコ製品は現在のところ見つかっていません。

詳細

Cisco 適応型セキュリティ アプライアンス（ASA）は、シスコ クライントレス VPN ソリューションと呼ばれる機能を搭載しています。シスコ クライントレス VPN 機能により、ユーザは Web ブラウザを使用してエンドポイント デバイスから Cisco ASA デバイスに SSL VPN トンネルを作成することができます。接続されると、ASA は複数の ActiveX および Java アプリケーションをエンドポイント デバイスにプッシュするため、多くの機能の運用が可能になります。

Microsoft ActiveX テクノロジーをサポートするブラウザを使用してクライントレス VPN トンネルを作成すると、ブラウザを実行しているエンドポイントのシステムに Cisco Port Forwarder ActiveX コントロールが送信される可能性があります。このコントロールには悪用され得るバッファ オーバーフローの脆弱性が含まれ、リモートの認証されていない攻撃者が悪意のある Web サイトをユーザに訪問させ、攻撃者が管理する任意のコードをエンドポイント デバイスで実行できる可能性があります。攻撃者のコードは、その攻撃者の管理する Web サイトの訪問に使用されたブラウザを起動したユーザの権限で実行されます。ユーザが管理者権限を持っている場合、完全な侵害が可能になる場合があります。

修正されたコントロールを含むソフトウェア バージョンに Cisco ASA デバイスをアップグレードしても、影響を受けるコントロールをダウンロードしたエンドポイントのシステムでは問題が修正されません。影響を受けるエンドポイント システムは、このアドバイザリの「回避策」のセクションに示されている対策のいずれかによって、コントロールを無効にする必要があります。またエンドポイント システムは、シスコ クライントレス VPN ソリューションを介して、修正されたコントロールを含むソフトウェアのバージョンを実行している Cisco ASA デバイスに接続し、影響を受けないバージョンのコントロールに更新することもできます。

影響を受けるコントロールは、エンドポイントのシステムに読み込まれたとき、 *cscopf.ocx* というバイナリ名を持ち、CLSID **{B8E73359-3422-4384-8D27-4EA1B4C01232}** としてシステムに登録されます。 *cscopf.ocx* コントロールの修正版は、CLSID **{C861B75F-EE32-4aa4-B610-281AF26A8D1C}** として登録されます。

Microsoft はシスコからの依頼により、影響を受けるコントロールに対するグローバル キルビットを設定しました。このキルビットを含む Microsoft update の詳細は Microsoft Knowledge Base article 2695962 に記述され 2012 年 5 月 8 日にリリースされています。Microsoft Security Advisory は以下のリンクで確認できます: Microsoft Security Advisory (2695962) Update Rollup for ActiveX Kill Bits

自動・手動に関わらず、一旦このアップデートを適用すると、影響を受けるコントロールはエンドポイントで機能しなくなります。

このアドバイザリは、Cisco Port Forwarder ActiveX コントロールにおける脆弱性に対するものです。これは、シスコ クライントレス VPN 機能が使用されるときに Cisco ASA によって提供されるものです。この脆弱性は Cisco bug ID CSCtr00165（ 登録ユーザのみ ）として文書化され、Common Vulnerabilities and Exposures (CVE) ID CVE-2012-0358 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

CSCtr00165, Cisco Clientless VPN Port Forwarder ActiveX Control Remote Code Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **9.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - **7.7**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、リモートの認証されていない攻撃者は、Web ブラウザを起動したユーザの権限によって、影響を受けるエンドユーザ システム上で任意のコードを実行できる可能性があります。ユーザが管理者権限を持っている場合、コードの実行はシステムの完全な改ざんにつながる可能性があります。

ソフトウェア バージョンおよび修正

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 アーカイブと、後続のアドバイザリを参照して、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。情報が不明確な場合は、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。

Affected Version	First Fixed Release	Recommended Release
Cisco ASA 7.0	Not Vulnerable	Migrate to 7.2 or later
Cisco ASA 7.1	Vulnerable	Vulnerable; Migrate to 7.2 or later
Cisco ASA 7.2	7.2(5.6)	7.2(5.7)
Cisco ASA 8.0	8.0(5.26)	Migrate to 8.2(5.26) or later
Cisco ASA 8.1	8.1(2.53)	Migrate to 8.2(5.26) or later
Cisco ASA 8.2	8.2(5.18)	8.2(5.26)
Cisco ASA 8.3	8.3(2.28)	Migrate to 8.4(3.8) or later
Cisco ASA 8.4	8.4(2.16)	8.4(3.8)
Cisco ASA 8.5	Not Vulnerable	8.5(1.7)
Cisco ASA 8.6	8.6(1.1)	8.6(1.1)

注： Cisco ASA ソフトウェア バージョン 7.0 および 7.1 はソフトウェア メンテナンスが終了しています。Cisco ASA ソフトウェア バージョン 7.0 または 7.1 をご利用のお客様は、サポートされている Cisco ASA ソフトウェア バージョンへのアップグレードに関してシスコ サポート チームにお問い合わせください。

注：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たすべての脆弱性に対する修正が含まれています。シスコはこれら推奨リリース、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。

注：修正されたバージョンの Cisco Port Forwarder ActiveX コントロール を含むソフトウェア バージョンに Cisco ASA デバイスをアップグレードしても、影響を受けるエンドポイントのシステムの脆弱性は削除されません。影響を受けるエンドポイント システムは、シスコ クライントレス Web ソリューションを介して、修正されたソフトウェアを実行している Cisco ASA デバイスに接続し、修正されたバージョンをダウンロードするか、このアドバイザリの「回避策」のセクションに示されている対策のいずれかによって該当するコントロールを無効にする必要があります。

回避策

エンド ユーザまたは管理者は、該当する ActiveX コントロールに対するキル ビットを設定することで、Internet Explorer への攻撃を緩和できます。これは、影響を受けるマシン上で直接、ある

いは Active Directory Group Policy を通して、レジストリを変更することにより実行できます。

警告： Microsoft Windows ベースのデバイスのシステム レジストリを誤って変更すると、重大な問題を引き起こすことがあります。シスコまたは Microsoft のいずれも、*.reg* ファイルによるレジストリ変更の適用、またはレジストリ エディタを誤って使用したことによる不適切なレジストリ変更に起因する問題を解決できることを保証いたしません。システムのレジストリの変更はユーザの責任で行なってください。

値が **{B8E73359-3422-4384-8D27-4EA1B4C01232}** の CLSID に対するキル ビットの設定は、Notepad などのテキスト エディタに次のテキストを貼り付けます。*.reg* のファイル拡張子を使用して、ファイルを保存します。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet Explorer¥ActiveX
Compatibility¥{B8E73359-3422-4384-8D27-4EA1B4C01232}]
"Compatibility Flags"=dword:04000400

[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Internet
Explorer¥ActiveX Compatibility¥{B8E73359-3422-4384-8D27-
4EA1B4C01232}]
"Compatibility Flags"=dword:04000400
```

エンド ユーザはこの *.reg* ファイルをダブルクリックすることで、個別のシステムに適用することができます。管理者は Group Policy を使用してドメイン全体にレジストリの変更を適用することもできます。Group Policy の使用については、次の Microsoft TechNet 記事で詳細に説明されています。Group Policy Collection

レジストリの変更を適用した後、Microsoft Internet Explorer を再起動して変更を有効にする必要があります。キル ビットが設定されると、Cisco クライントレス VPN システムまたは Internet Explorer によってアクセスされた悪意のある Web ページから該当するコントロールにはアクセスできなくなります。この変更は、Cisco Port Forwarder ActiveX コントロールを使用する一部のクライアントレスの展開に影響を与えることがあります。動作が停止する可能性のある一般的なコンポーネントの 1 つが ActiveX RDP プラグインです。

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。
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20120314-asaclient

注： 上記の回避策を適用したエンドポイント デバイスに修正済み ActiveX コントロールまたは Microsoft キル ビット アップデートを適用した場合、レジストリのキル ビットの値は 0x04000400 から 0x00000400 に変わります。この変更が行われても、影響を受ける ActiveX コントロールの実行ブロックは有効です。上記のレジストリ変更は ActiveX キル ビットに加え、バイナリ ビヘイビア キル ビットも設定しています。バイナリ ビヘイビア キル ビットは、Windows Server 2003 以上でサポートされ、追加の保護機能を提供できます。バイナリ ビヘイビア キル ビットをサポートしていないプラットフォームはこの設定を無視し、ActiveX キル ビットのみを使用します。

修正済みソフトウェアの入手

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 アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の

問題に関してご確認ください。

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、ご購入いただいたフィーチャ セットに対してのみとなります。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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html または http://www.cisco.com/public/sw-center/sw-usingswc.shtml 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。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Center からアップグレードを入手することができます。http://www.cisco.com

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、適切な処置について支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策または修正が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

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 Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC を通して無償アップグレードをお求めください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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不正利用事例とその公表は確認しておりません。

この脆弱性は、CERT/CC の Will Dormann 氏によってシスコに報告されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asaclient

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.1	2012-May-15	Added information about the Microsoft Global Kill Bit update release on May 8th, 2012
Revision 1.0	2012-Mar-14	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。