Cisco IOS Software SSL VPN Denial of Service Vulnerability

Advisory ID: cisco-sa-20140326-ios-sslvpn

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ios-sslvpn

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 1.0

For Public Release 2014 March 26 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアの Secure Sockets Layer（SSL）VPN サブシステムの脆弱性により、認証されていないリモートの攻撃者によってサービス拒否（DoS）状態が引き起こされる可能性があります。

この脆弱性は、特定のタイプの HTTP 要求の処理の失敗によるものです。攻撃者はこの脆弱性を不正利用し、該当デバイスのメモリを消費するよう巧妙に設計された要求を送信する可能性があります。不正利用により、攻撃者が該当デバイス上のメモリを消費し、断片化させる可能性があります。これによりパフォーマンスが低下し、特定のプロセスに失敗したり、該当デバイスが再起動したりする可能性があります。

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。この脆弱性を軽減する回避策はありません。

このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ios-sslvpn

注：2014 年 3 月 26 日の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には 6 件の Cisco Security Advisory が含まれています。これらのアドバイザリはすべて、Cisco IOS ソフトウェアの脆弱性に対処するものです。各 Cisco IOS ソフトウェア セキュリティ アドバイザリには、そのアドバイザリで詳述された脆弱性を修正する Cisco IOS ソフトウェア リリース、および 2014 年 3 月にバンドル公開したすべての Cisco IOS ソフトウェアの脆弱性を修正する Cisco IOS ソフトウェア リリースを記載しています。

個別の公開リンクは、次のリンクにある「*Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication*」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html

該当製品

脆弱性が認められる製品

WebVPN 拡張機能（Cisco IOS SSLVPN）が設定されたデバイスのみが、この脆弱性の影響を受けます。

デバイスで WebVPN が有効になっているかどうかは、 **show webvpn gateway** EXEC コマンドを発行することで確認できます。脆弱性が認められるソフトウェアを実行すると、デバイスが影響を受け、 *起動*するよう設定されたゲートウェイの *管理*および *運用*ステータスが一覧表示されます。

次の例では、デバイスに単一の WebVPN ゲートウェイ（ *ssl-vpn* ）が設定されています。このゲートウェイは起動し、接続を受け入れます。

```
Router#show webvpn gateway

Gateway Name                        Admin  Operation
------------ ----- ---------
ssl-vpn up up
```

管理者は、 **show running-config | include webvpn** という EXEC コマンドを発行することで、設定を確認できます。デバイスから何らかの出力があれば、SSLVPN が設定されており、そのデバイスには脆弱性が存在する可能性があります。 **show running-config | include webvpn** からの出力に *webvpn gateway <word>* が含まれている場合、そのデバイスでは Cisco IOS SSLVPN 機能が設定されています。 *webvpn gateway* セクションが 1 つでも *inservice* コマンドを含んでいる場合、そのデバイスには脆弱性が存在します。次の例は、Cisco IOS SSLVPN が設定された脆弱性のあるデバイスを示しています。

```
Router# show running-config | include webvpn

webvpn gateway ssl-vpn
ip address 10.1.1.1 port 443
ssl trustpoint Gateway-TP
inservice
!
Router#
```

WebVPN ゲートウェイが設定されていない場合や、設定されているすべての WebVPN ゲートウェイ エントリの WebVPN ゲートウェイ セクションに *no inservice* サブコマンドが含まれる場合は、Cisco IOS SSLVPN をサポートするデバイスに脆弱性はありません。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログイ

ンし **show version** コマンドを実行してシステム バナーを表示させます。「Internetwork Operating System Software」、「Cisco IOS Software」あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。その後ろにイメージ名が括弧の間に表示され、続いてバージョンと Cisco IOS ソフトウェア リリース名が表示されます。他のシスコ デバイスでは、**show version** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.2(4)M5 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_teamRouter> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

Cisco IOS ソフトウェア リリースの命名規則の追加情報は、ホワイト ペーパー「Cisco IOS and NX-OS Software Reference Guide」で確認できます。

脆弱性が認められない製品

Cisco IOS XE ソフトウェアは、この脆弱性の影響を受けません。

Cisco IOS XR ソフトウェアは、この脆弱性の影響を受けません。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、この脆弱性の影響を受けません。

他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

Cisco IOS の SSL VPN でのサービス拒否攻撃に対する脆弱性

Cisco IOS ソフトウェアの Secure Sockets Layer（SSL）VPN サブシステムの脆弱性により、認証されていないリモートの攻撃者によってサービス拒否（DoS）状態が引き起こされる可能性があります。

この脆弱性は、特定のタイプの HTTP 要求の処理の失敗によるものです。攻撃者はこの脆弱性を不正利用し、該当デバイスのメモリを消費するよう巧妙に設計された要求を送信する可能性があります。不正利用により、攻撃者が該当デバイス上のメモリを消費し、断片化させる可能性があります。これによりパフォーマンスが低下し、特定のプロセスに失敗したり、該当デバイスが再起動したりする可能性があります。
該当デバイスへのそれぞれの不正な接続に対して、3 ウェイ TCP ハンドシェイクを完了する必要があります。ただし、認証は必須ではありません。 SSLVPN のデフォルト TCP ポート番号は 443 です。
この脆弱性は、Cisco Bug ID CSCuf51357（ 登録ユーザ専用 ）として文書化され、Common

Vulnerabilities and Exposures（CVE）ID として CVE-2014-2112 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ 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。

シスコでは、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知ることができます。

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

またシスコでは、各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/

Cisco IOS SSL VPN Denial of Service Vulnerability - CSCuf51357 Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

本ドキュメントで説明されている脆弱性を不正利用することで、認証されていないリモートの攻撃者が DoS 状態を発生させる可能性があります。これによって、該当デバイスのパフォーマンスの低下や、ルーティング プロトコルの維持の失敗、デバイスの再起動が発生するおそれがあります。

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起

こりうる障害を判断し、それに対応できるアップグレード 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、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。

2014 年 2 月に、シスコは 2005 ～ 2010 年の間に製造されたメモリ コンポーネントに関する業界全体の問題の詳細を発表しました。これらのコンポーネントを使用しているシスコ製品の大多数は、フィールドでの故障発生率が予想レベルを下回りました。ただし、デバイスのリロードや電源の再投入を行うと、コンポーネントに障害が発生する可能性があります。また、この問題に関連するセキュリティへの影響はまだ認められていませんが、当該製品のサブセットでは、ソフトウェア アップグレード プロセス中にメモリ コンポーネント エラーが発生する可能性もあります。アップグレードを決定する前に、関連情報および製品固有の Field Notice（www.cisco.com/go/memory）を確認することを推奨します。各 Field Notice には、ソフトウェア アップグレード中にその製品でメモリ コンポーネントの障害が発生するかどうかが記載されています。**Cisco IOS ソフトウェア**Cisco IOS ソフトウェア チェッカーを使用すれば、Cisco IOS ソフトウェアの脆弱性により起こりうる障害をすばやく判断できます。このツールによって、特定の Cisco IOS ソフトウェア リリースに影響を与えるシスコのセキュリティ アドバイザリをすばやく特定できます。ドロップダウン メニューからリリースを選択するか、ローカル システムからファイルをアップロードすることで、検索を開始できます。このツールには、**show version** コマンド出力の解析機能もあります。以前に公開されているシスコの全セキュリティ アドバイザリ、特定の公開情報、2014 年 3 月のバンドル公開を検索することによって、結果をカスタマイズできます。

また、次の Cisco IOS ソフトウェアの表を使用して、影響を確認することもできます。各行が Cisco IOS ソフトウェア リリースに対応しています。特定のリリースに脆弱性がある場合は、修正が含まれている最初のリリースが 2 番目の列に記載されています。3 列目には、この Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開のすべての脆弱性を修正する最初のリリースが記載されています。

ソフトウェアの修正情報の詳細を表示

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2014 Bundled Publication
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2014 Bundled Publication
There are no affected 12.2-based releases		
Affected 12.3-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2014 Bundled Publication
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2014 Bundled Publication
There are no affected 12.4 based releases		
Affected 15.0-Based	First Fixed Release	First Fixed Release for All Advisories in the March 2014 Bundled Publication

Releases		
There are no affected 15.0 based releases		
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2014 Bundled Publication**
15.1EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
15.1GC	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.1M	15.1(4)M7	15.1(4)M8; Available on 26-MAR-14
15.1MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1MRA	Not vulnerable	15.1(3)MRA3
15.1S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Vulnerable; First fixed in Release 15.2S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(2)SG4; Available on 04-JUN-14 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SY	Not vulnerable	15.1(1)SY3; Available on 28-MAR-14 15.1(2)SY2
15.1T	Vulnerable; First fixed in Release 15.1M Releases up to and including 15.1(1)T5 are not vulnerable.	Vulnerable; First fixed in Release 15.1M
15.1XO	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2014 Bundled Publication**
15.2E	Not vulnerable	15.2(1)E2
15.2EX	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2EY	Not vulnerable	Vulnerable; First fixed in Release 15.2E
15.2GC	15.2(4)GC1	15.2(4)GC1
15.2JA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2JAX	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2JB	Not vulnerable	15.2(4)JB3s 15.2(4)JB4
15.2JBX	Not vulnerable	Vulnerable; contact your support organization per

		the instructions in Obtaining Fixed Software section of this advisory.
15.2JN	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2M	15.2(4)M6; Available on 26-MAR-14	15.2(4)M6; Available on 26-MAR-14
15.2S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(4)S5 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.2SA	Not vulnerable	Not vulnerable
15.2SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2SNI	Not vulnerable	Vulnerable; First fixed in Release 15.3S
15.2T	Vulnerable; First fixed in Release 15.2M	Vulnerable; First fixed in Release 15.2M
Affected 15.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2014 Bundled Publication**
15.3M	15.3(3)M2	15.3(3)M2
15.3S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.3(3)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.3T	15.3(1)T4; Available on 30-MAY-14 15.3(2)T3	15.3(2)T3
Affected 15.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2014 Bundled Publication**
15.4CG	Not vulnerable	Not vulnerable
15.4S	Releases prior to 15.4(1)S1 are vulnerable; Releases 15.4(1)S1 and later are not vulnerable. Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Releases prior to 15.4(1)S2 are vulnerable; Releases 15.4(1)S2 and later are not vulnerable. Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.4T	15.4(1)T1	15.4(1)T1

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアは、2014 年 3 月の Cisco IOS Software Security Advisory バンドル公開に含まれている脆弱性の影響を受けません。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2014 年 3 月の Cisco IOS Software Security Advisory バンドル公開に含まれている脆弱性の影響を受けません。

回避策

このシスコ セキュリティ アドバイザリで説明された脆弱性に回避策はありません。

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の特有の問題をご確認ください。

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。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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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。

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 Navigator 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/cisco/software/navigator.html

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、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、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に関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象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ことを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- Eメール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

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（ http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html ）を参照してください。

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、カスタマー ケースの調査時に、Cisco TAC によって発見されたものです。

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-20140326-ios-sslvpn

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

本アドバイザリに関する今後の更新は 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。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-March-26	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サポート、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の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。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。