Cisco IOSソフトウェア WebVPN および SSLVPN 脆弱性

High	**アドバイザリーID :** cisco-sa-20090325-webvpn **初公開日 :** 2009-03-25 16:00 **バージョン 1.3 :** Final **CVSSスコア :** 7.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCsx28420 CSCsx15333 CSCsl30548 CSCsx28406	CVE-2009-0626

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 IOSソフトウェアはサービス拒否状態を引き起こすのに認証なしでリモートで不正利用することができる Cisco IOS WebVPN または Cisco IOS SSL VPN 機能（SSLVPN）内の 2 脆弱性が含まれています。 脆弱性は両方とも Cisco IOS WebVPN および Cisco IOS SSL VPN 両方機能に影響を与えます:

1. 巧妙に細工された HTTPS パケットはデバイスをクラッシュします。
2. SSLVPN セッション原因デバイスのメモリリーク。

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。

これらの脆弱性を軽減する回避策がありません。

このアドバイザリは次のリンクに掲載されます: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn。

注: 2009 年 3月 25 日、Cisco IOS セキュリティ アドバイザリによって組み込まれる書は 8 つのセキュリティ アドバイザリが含まれています。 アドバイザリすべては Cisco IOSソフトウェアの脆弱性に対処します。 各アドバイザリはリリースをリストしますアドバイザリの脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCP サービス拒否の脆弱性

325-ctcp
- Cisco IOSソフトウェア倍数は IP ソケット脆弱性を特色にします http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip
- Cisco IOSソフトウェア モバイル IP およびモービル IPv6 脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip
- Cisco IOSソフトウェア Secure Copy（SCP） 特権 拡大脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp
- Cisco IOSソフトウェア Session Initiation Protocol（SIP） サービス拒否の脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip
- Cisco IOSソフトウェア複数の機能によって細工 される TCP シーケンス脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp
- Cisco IOSソフトウェア複数の機能 巧妙に細工された UDP パケットの脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp
- Cisco IOSソフトウェア WebVPN および SSLVPN 脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

脆弱性のある製品

Cisco IOSソフトウェアの実行するデバイスによって影響を受けるバージョンは SSLVPN と影響を受けていますもし設定するなら。

Cisco製品で動作している Cisco IOS ソフトウェア リリース、管理者をログイン判別し、システムバナーを表示する **" show version " コマンドを**発行することはデバイスにできます。 "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 "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Ciscoデバイスに**" show version " コマンドが**ありませんし、別の出力を提供しないかもしれません。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

以下の例は、Cisco 製品にて、IOSリリース 12.4(20)T が稼動し、そのイメージ名が C1841-ADVENTERPRISEK9-M であることを示しています:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/warp/public/620/1.html。

SSLVPN がデバイスで、デバイスへのログイン判別し有効に なる、Command Line Interface （CLI）コマンド「発行するため **show running-config** ことを **| webvpn を」含んで下さい**。 デバイスが出力されるあらゆる戻せばこれは SSLVPN がデバイスで設定され、デバイスが脆弱かもしれないことを意味します。 脆弱 な コンフィギュレーションはデバイスが Cisco IOS WebVPN （リリース 12.3(14)T で導入される）または Cisco IOS SSL VPN をサポートしているかどうかによって変わります（リリース 12.4(6)T で導入される）。 次のメソッドはデバイスが脆弱であるかどうか確認する方法を記述します:

「show running-config からの出力 **| webvpn を」**含まれています**「webvpn イネーブルが含んで下さい」**それからデバイスがオリジナル Cisco IOS WebVPN で設定される。 デバイスを確認する唯一の方法は脆弱 webvpn がコマンド**「webvpn イネーブル」**によって有効に なること、そして**「ssl トラストポイント」が**設定されたことを確認するために**「show running-config」**の出力を検査することですです。 次の例は Cisco IOS WebVPN で設定される脆弱 なデバイスを示したものです:

```
webvpn enable
!
webvpn
 ssl trustpoint TP-self-signed-29742012
```

「show running-config からの出力 **| webvpn を」**含まれています**「webvpn ゲートウエイ *<word>* が含んで下さい」**それからデバイスが Cisco IOS SSL VPN 機能をサポートしている。 デバイスは**「webvpn ゲートウエイ」**セクションがの少なくとも 1 つで**「インサービス"**コマンドある場合脆弱です。 次の例は Cisco IOS SSL VPN で設定される脆弱 な デバイスを示したものです:

```
Router# show running | section webvpn
webvpn gateway Gateway
 ip address 10.1.1.1 port 443
 ssl trustpoint Gateway-TP
 inservice
 !
Router#
```

Cisco IOS SSL VPN をサポートするデバイスは**「インサービス」**「webvpn ゲートウエイ」コマンドが含まれていることを設定される「webvpn ゲートウエイ」か「webvpn ゲートウエイ」設定されるすべてのない場合脆弱ではないです。

脆弱性を含んでいないことが確認された製品

以下の製品はこの脆弱性から影響を受けません:

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco IOS XR ソフトウェア
- Cisco IOS XE ソフトウェア

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 SSLVPN 機能はどこでもインターネットからのユーザによって企業サイトへのリモート アクセスを提供します。 SSLVPN は特定のエンタープライズ アプリケーションに安全なアクセスをそれらは VPN クライアント ソフトウェアがあるように要求しないでエンドユーザデバイスでインストールされるユーザに、E メールおよび Web ブラウジングのような、与えます。

WebVPN 拡張は（Cisco IOS SSL VPN）、Cisco IOS Release 12.4(6)T でリリースされて、廃止しますコマンドを特色になり、コンフィギュレーションは Cisco IOS WebVPN で最初に提言しました。

Cisco IOS WebVPN についてのより詳しい 情報は次のリンクで「Cisco IOS ソフトウェア リリース 12.3T WebVPN 機能ガイド」で利用できます:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/g_sslvpn.html

Cisco IOS SSL VPN についてのより詳しい 情報は次のリンクで「Cisco IOS ソフトウェア リリース 12.4T SSLVPN 機能ガイド」で利用できます:
http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html

システム ソフトウェアの影響を受けたバージョンを実行している Cisco IOSデバイスのこれら二つの脆弱性に関する詳細は次のとおりです:

巧妙に細工された HTTPS パケットはデバイスをクラッシュします

SSLVPN のために設定されるデバイスは特別に 巧妙に細工された HTTPS パケットを受信するときリロードするか、またはハングするかもしれません。 認証が**「ない」**必須であるどんなに脆弱性が正常に不正利用されることができるように SSLVPN 機能の関連する TCPポート番号への三方ハンドシェイクの完了が必要となります。 SSLVPN のためのデフォルト TCPポート番号は 443 です。

この脆弱性は Cisco バグ ID CSCsk62253 （**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）識別子 CVE-2009-0626 はこの脆弱性に割り当てられました。

SSLVPN セッション原因デバイスのメモリリーク

SSLVPN のために設定されるデバイスは異常に切断された SSL セッションを処理するとき伝達

コントロール ブロック（TCBs）をリークさせるかもしれません。 継続的不正利用はメモリ リソースを枯渇させるデバイスという結果に終り、デバイスのクラッシュという結果に終るかもしれません。 認証が「」この脆弱性を不正利用するために必要となりません。

メモリリークは次の例ののようなコマンド「**show tcp 要約**」の、実行によって検出することができます:

```
Router#show tcp brief
TCB        Local Address      Foreign Address     (state)
468BBDC0  192.168.0.22.443   192.168.0.33.19794   CLOSEWAIT
482D4730  192.168.0.22.443   192.168.0.33.22092   CLOSEWAIT
482779A4  192.168.0.22.443   192.168.0.33.16978   CLOSEWAIT
4693DEBC  192.168.0.22.443   192.168.0.33.21580   CLOSEWAIT
482D3418  192.168.0.22.443   192.168.0.33.17244   CLOSEWAIT
482B8ACC  192.168.0.22.443   192.168.0.33.16564   CLOSEWAIT
46954EB0  192.168.0.22.443   192.168.0.33.19532   CLOSEWAIT
468BA9B8  192.168.0.22.443   192.168.0.33.15781   CLOSEWAIT
482908C4  192.168.0.22.443   192.168.0.33.19275   CLOSEWAIT
4829D66C  192.168.0.22.443   192.168.0.33.19314   CLOSEWAIT
468A2D94  192.168.0.22.443   192.168.0.33.14736   CLOSEWAIT
4688F590  192.168.0.22.443   192.168.0.33.18786   CLOSEWAIT
4693CBA4  192.168.0.22.443   192.168.0.33.12176   CLOSEWAIT
4829ABC4  192.168.0.22.443   192.168.0.33.39629   CLOSEWAIT
4691206C  192.168.0.22.443   192.168.0.33.17818   CLOSEWAIT
46868224  192.168.0.22.443   192.168.0.33.16774   CLOSEWAIT
4832BFAC  192.168.0.22.443   192.168.0.33.39883   CLOSEWAIT
482D10CC  192.168.0.22.443   192.168.0.33.13677   CLOSEWAIT
4829B120  192.168.0.22.443   192.168.0.33.20870   CLOSEWAIT
482862FC  192.168.0.22.443   192.168.0.33.17035   CLOSEWAIT
482EC13C  192.168.0.22.443   192.168.0.33.16053   CLOSEWAIT
482901D8  192.168.0.22.443   192.168.0.33.16200   CLOSEWAIT
```

上記の出力では状態のそれらの伝達 コントロール ブロック（TCBs）は CLOSEWAIT なくならなかったりし、メモリリークを表します。 以下の事項に注意して下さい: 443 の口ーカル TCPポートの TCP 接続だけ（HTTPS のためのよく知られたポート）関連しています。

この脆弱性は Cisco バグ ID **CSCsw24700**（**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）識別子 CVE-2009-0628 はこの脆弱性に割り当てられました。

セキュリティ侵害の痕跡

回避策

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。

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。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	**修正済みリリースの入手可能性**	
Affected 12.0-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.0 ベースのリリースはありません。		
Affected 12.1-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.1 ベースのリリースはありません。		
Affected 12.2-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.2 基づいたリリースがありません		
Affected 12.3-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.3	脆弱性なし	
12.3B	脆弱性なし	
12.3BC	脆弱性なし	
12.3BW	脆弱性なし	
12.3EU	脆弱性なし	
12.3JA	脆弱性なし	
12.3JEA	脆弱性なし	

12.3JEB	脆弱性なし	
12.3JEC	脆弱性なし	
12.3JK	脆弱性なし	
12.3JL	脆弱性なし	
12.3JX	脆弱性なし	
12.3T	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.3TPC	脆弱性なし	
12.3VA	脆弱性あり; contact TAC	
12.3XA	脆弱性なし	
12.3XB	脆弱性なし	
12.3XC	脆弱性なし	
12.3XD	脆弱性なし	
12.3XE	脆弱性なし	
12.3XF	脆弱性なし	
12.3XG	脆弱性なし	
12.3XI	脆弱性なし	
12.3XJ	脆弱性なし	
12.3XK	脆弱性なし	
12.3XL	脆弱性なし	
12.3XQ	脆弱性なし	
12.3XR	脆弱性なし	
12.3XS	脆弱性なし	
12.3XU	脆弱性なし	
12.3XW	脆弱性なし	
12.3XX	脆弱性なし	
12.3XY	脆弱性なし	
12.3XZ	脆弱性なし	
12.3YA	脆弱性なし	
12.3YD	脆弱性なし	
12.3YF	脆弱性なし	
12.3YG	脆弱性なし	
12.3YH	脆弱性なし	
12.3YI	脆弱性なし	
12.3YJ	脆弱性なし	
12.3YK	Release prior to 12.3(11)YK3 are vulnerable， releases 12.3(11)YK3 and later are not vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.3YM	脆弱性なし	

12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YS	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YU	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YX	脆弱性なし	
12.3YZ	脆弱性なし	
12.3ZA	脆弱性なし	
Affected 12.4-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	12.4(16)MR	12.4(19)MR2
12.4SW	脆弱性なし	
12.4T	12.4(15)T7 12.4(20)T 12.4(15)T9; 29-APR-2009 で利用可能	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利

		用可能
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XB	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XC	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XD	12.4(4)XD12; 27-MAR-2009 で利用可能	12.4(4)XD 12; 27-MAR-2009 で利用可能
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XK	脆弱性なし	
12.4XL	脆弱性なし	
12.4XM	脆弱性なし	
12.4XN	脆弱性なし	
12.4XP	脆弱性あり; contact TAC	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XV	脆弱性あり; contact TAC	
12.4XW	12.4(11)XW10	12.4(11)X W10
12.4XY	12.4(15)XY4	12.4(22)T1

12.4XZ	12.4(15)XZ1	12.4(15)XZ2
12.4YA	脆弱性なし	
12.4YB	脆弱性なし	
12.4YD	脆弱性なし	

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

これらの脆弱性はカスタマー サポートを処理するとき呼出します検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

改訂履歴

リビジョン 1.3	2009-June-26	March/09 によって結合される修正済みソフトウェア 表への取除かれた参照。
リビジョン 1.2	2009-June-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。
リビジョン 1.1	2009-May-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。
リビジョン 1.0	2009-March-25	Initial public release.

利用規約