Cisco IOSソフトウェアのWebVPNおよびSSLVPNの脆弱性

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ソフトウェアには、Cisco IOS WebVPNまたはCisco IOS SSLVPN機能(SSLVPN)に含まれる2つの脆弱性があり、認証なしでリモートから悪用されてサービス妨害(DoS)状態が発生する可能性があります。どちらの脆弱性も、Cisco IOS WebVPN機能とCisco IOS SSLVPN機能の両方に影響します。

1. 巧妙に細工されたHTTPSパケットによってデバイスがクラッシュする
2. SSLVPNセッションが原因で、デバイスでメモリリークが発生します。

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、次のリンクに掲載されます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn。

注：2009年3月25日のCisco IOSセキュリティアドバイザリバンドル公開には8件の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。各アドバイザリには、そのアドバイザリに記載された脆弱性を修正するリリースが記載されています。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCPのDoS脆弱性

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ctcp
- Cisco IOSソフトウェアの複数の機能におけるIPソケットの脆弱性
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip
- Cisco IOSソフトウェアモバイルIPおよびモバイルIPv6の脆弱性
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip
- Cisco IOSソフトウェアのSecure Copyにおける権限昇格の脆弱性
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp
- Cisco IOSソフトウェアのSession Initiation ProtocolにおけるDoS脆弱性
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip
- Cisco IOSソフトウェアの複数の機能における巧妙に細工されたTCPシーケンスの脆弱性
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp
- Cisco IOSソフトウェアの複数機能における巧妙に細工されたUDPパケットの脆弱性
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp
- Cisco IOSソフトウェアのWebVPNおよびSSLVPNの脆弱性
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

脆弱性のある製品

該当するバージョンのCisco IOSソフトウェアを実行しているデバイスは、SSLVPNが設定されている場合に該当します。

シスコ製品で実行されているCisco IOSソフトウェアリリースは、管理者がデバイスにログインして、show versionコマンドを発行することにより確認できます。"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。他のシスコデバイスには「show version」コマンドがないか、異なる出力が表示される場合があります。

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 (fc
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ソフトウェアのリリース命名規則の追加情報は、次のリンクの「White Paper: Cisco IOS Reference Guide」で確認できます。http://www.cisco.com/warp/public/620/1.html。

デバイスでSSLVPNが有効になっていることを確認するには、デバイスにログインして、コマンドラインインターフェイス(CLI)でshow running-config | include webvpn"を実行します。デバイスから何らかの出力が返された場合、そのデバイスには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。脆弱性のある設定は、デバイスがCisco IOS WebVPN(リリース12.3(14)Tで導入)またはCisco IOS SSLVPN(リリース12.4(6)Tで導入)のどちらをサポートしているかによって異なります。次に、デバイスに脆弱性が存在するかどうかを確認する方法を示します。

「show running-config | include webvpn"に"webvpn enable"が含まれている場合、デバイスは元のCisco IOS WebVPNで設定されています。デバイスが脆弱であることを確認する唯一の方法は、「show running-config」の出力を調べ、webvpnがコマンド「webvpn enable」によって有効になっており、「ssl trustpoint」が設定されていることを確認することです。次の例は、Cisco IOS WebVPNが設定された脆弱性のあるデバイスを示しています。

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

「show running-config | include webvpn"に"webvpn gateway <word>"が含まれている場合、そのデバイスはCisco IOS SSLVPN機能をサポートしています。「webvpn gateway」セクションの少なくとも1つに「inservice」コマンドがある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 | section webvpn
webvpn gateway Gateway
 ip address 10.1.1.1 port 443
 ssl trustpoint Gateway-TP
 inservice
 !
Router#
```

Cisco IOS SSLVPNをサポートするデバイスに「webvpn gateways」が設定されていない場合、または設定されているすべての「webvpn gateways」に「no inservice」の「webvpn gateway」コマンドが含まれている場合は、この脆弱性は存在しません。

脆弱性を含んでいないことが確認された製品

次の製品は、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
- 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、ユーザがインターネット上のどこからでも企業サイトにリモートアクセスできるようにします。SSLVPNを使用すると、エンドユーザのデバイスにVPNクライアントソフトウェアをインストールしなくても、電子メールやWeb閲覧などの特定のエンタープライズアプリケーションに安全にアクセスできます。

WebVPN拡張機能(Cisco IOS SSLVPN)は、Cisco IOSリリース12.4(6)Tでリリースされ、Cisco IOS WebVPNで最初に使用されていたコマンドと設定を廃止します。

Cisco IOS WebVPNの詳細については、次のリンクの『Cisco IOS Software Release 12.3T WebVPN feature guide』を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/g_sslvpn.html

Cisco IOS SSLVPNの詳細については、次のリンクの『Cisco IOS Software Release 12.4T SSLVPN feature guide』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html

影響を受けるバージョンのシステムソフトウェアを実行しているCisco IOSデバイスにおけるこれら2つの脆弱性の詳細は次のとおりです。

巧妙に細工されたHTTPSパケットによってデバイスがクラッシュする

SSLVPN用に設定されたデバイスは、特別に巧妙に細工されたHTTPSパケットを受信すると、リロードまたはハングする可能性があります。この脆弱性を不正利用するには、SSLVPN機能の関連するTCPポート番号に対する3ウェイ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「不要」です。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 CSCsk62253(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-2009-0626が割り当てられています。

SSLVPNセッションが原因でデバイスのメモリリークが発生する

SSLVPN用に設定されたデバイスは、異常に切断されたSSLセッションの処理中に伝送制御ブロック(TCB)をリークする可能性があります。不正利用が続くと、デバイスのメモリリソースが枯渇し、デバイスがクラッシュ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認証は「不要」です。

メモリリークを検出するには、次の例のように、show tcp briefコマンドを実行します。

```
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、CLOSEWAIT状態のTransmission Control Block（TCB；伝送制御ブロック）は消えず、メモリリークを示しています。ローカルTCPポートが443（HTTPSの既知のポート）のTCP接続だけが関連することに注意してください。

この脆弱性は、Cisco Bug ID CSCsw24700(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-2009-0628が割り当てられています。

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

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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
影響を受ける 12.2 ベースのリリースはありません。		
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(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3TPC	脆弱性なし	
12.3VA	脆弱性あり。TACに連絡	
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	12.3(11)YK3より前のリリースには脆弱性があり、12.3(11)YK3以降のリリースには脆弱性はありません。最初の修正は12.4Tです。	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YM	脆弱性なし	
12.3YQ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YS	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YT	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）

12.3YU	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
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)（2009年6月5日に入手可能）	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
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（2009年4月29日に入手可能）	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XA	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XB	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XC	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XD	12.4(4)XD12（2009年3月27日に入手可能）	12.4(4)XD12（2009年3月27日に入手可能）
12.4XE	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年

		4月29日に入手可能）
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
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。TACに連絡	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XV	脆弱性あり。TACに連絡	

12.4XW	12.4(11)XW10	12.4(11)XW10
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	

推奨事項

$propertyAndFields.get("recommendations")

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コールの対応時に発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

改訂履歴

リビジョン 1.3	2009年 6月26日	2009年3月9日の統合修正済みソフトウェアテーブルへの参照を削除。
リビジョン	2009年 6月1日	リリース12.4(23a)の公開予定日を更新。

1.2		
リビジョン 1.1	2009年 5月1日	リリース12.4(23a)の公開予定日を更新。
リビジョン 1.0	2009年 3月25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。