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 :** Yes **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

修正済みソフトウェア

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。

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	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。