

Cisco IOS SSL VPN 脆弱性

High

アドバイザーID : cisco-sa-20100922-sslvpn

[CVE-2010-2836](#)

初公開日 : 2010-09-22 16:00

最終更新日 : 2012-09-21 19:17

バージョン 1.1 : Final

CVSSスコア : [7.8](#)

回避策 : [Yes](#)

Cisco バグ ID : [CSCtg21685](#)

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 Cisco IOS SSL VPN 機能が HTTP リダイレクトで設定されるとき脆弱性が含まれています。不正利用は遠隔により、非認証ユーザ新しい TCP 接続を保守するデバイスのリロード、不可能および他のサービス拒否 (DoS) 状態を引き起こすかもしれないメモリ枯渇状態という結果に終る可能性がある影響を受けたデバイスのメモリリークを引き起こすようにする可能性があります。

シスコはこ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ました。この脆弱性を軽減する回避策があります。

このアドバイザーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sslvpn> で掲示されます。

注: 2010 年 9 月 22 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 6 Cisco Security Advisory が含まれています。アドバイザーの 5 つは Cisco IOSソフトウェアの脆弱性に対処し、1 つのアドバイザーは Cisco Unified Communications Manager の脆弱性に対処します。各アドバイザーには、そのアドバイザーで詳述された脆弱性を解決するリリースを記載しています。次の URL リストの表は正しい 2010 年 9 月 22 日送達されたすべての Cisco IOSソフトウェア脆弱性、またはそれ以前ことリリースします:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-bundle>

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

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 SSL VPN および HTTPポート リダイレクションと脆弱もし設定するならば。

次のメソッドがデバイスが Cisco IOS SSL VPN のために設定され、脆弱であるかどうか確認するのに使用されるかもしれません:

show running-config からの出力 | **webvpn** を含まれています 「webvpn ゲートウェイ <word> 含んで下さい」 が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 ゲートウェイ」 セクションの少なくとも 1 つで **in service** コマンドがあれば、HTTPポート リダイレクションのために設定されます脆弱。 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
http-redirect port 80
ssl trustpoint Gateway-TP
in service
!
Router#
```

Cisco IOS SSL VPN をサポートするデバイスは 「webvpn ゲートウェイ」 が設定されない場合脆弱ではないです。

Cisco 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、機器にログインし **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 "Version" と Cisco IOS ソフトウェア リリース名が表示されます。 他の Cisco 機器では、**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 C2800NM-ADVSECURITYK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T を実行している Cisco製品を指定したものです:

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVSECURITYK9-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 22:00 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>

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 1.0	2010-September-22	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、単独の転載や意識を施した場合、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。