# SSL パケットを処理している間 Cisco IOS の脆弱性

High

**アドバイザリーID :** cisco-sa-20080924-ssl
**初公開日 :** 2008-09-24 16:00
**バージョン 1.1 :** Final
**CVSSスコア :** 7.8
**回避策 :** No Workarounds available
**Cisco バグ ID :** CSCsj85065

CVE-2008-3798

**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デバイスは SSL パケットを処理している間クラッシュするかもしれません。 これは SSL ベース セッションの終了の間に起こる場合があります。 おこるパケットは不正でし、パケット交換の一部として普通受け取られます。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。影響を受けたサービスをディセーブルにすることは別として、この脆弱性のエクスプロイトを軽減する利用可能 な 回避策がありません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl で掲示されます。

**注:** 2008 年 9月 24 日 IOS アドバイザリによって組み込まれる書は 12 のセキュリティ アドバイザリが含まれています。 アドバイザリの 11 は Cisco の IOS software の脆弱性に対処し、1 つのアドバイザリは Cisco Unified Communications Manager 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に説明がある脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosips
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip
- 924-cucm
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast
- 924-sccp
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosfw
- 924-l2tp

### 該当製品

## 脆弱性のある製品

実行するデバイス Cisco IOS および SSL ベース サービスを利用することはこの脆弱性に敏感です。 SSL を利用するいくつかのサービスは次のとおりです:

- **SSL 暗号化（HTTPS）をサポートする HTTPサーバ**
  次の例はディセーブルにされる標準 Cisco IOS HTTP サーバを備えている有効に なる SSL 有効に されて Cisco IOS HTTP サーバを示したものですデバイス:

```
Router#show running-config | include ip http
no ip http server
ip http secure-server
Router#
```

- **SSL 仮想 な プライベート ネットワーク（SSL VPN）別名 AnyConnect VPN**
  次の例は有効に なる SSL VPN 機能を備えているデバイスを示したものです:

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

- **パケット テレフォニー 機能のための Open Settlement Protocol（OSP）**
  次の例は有効に なる OSP 機能を備えている示し、HTTPS プロトコルを使用したものですデバイスを脆弱である:

```
Router#show running-config | include url
url https://<host_ip_address>:443/
Router#
```

Cisco IOS Bug Toolkit は正確にこのアドバイザリのための該当するリリースを反映しないかもしれません。 該当するリリースは次の通りです:

- 12.4(16)MR、12.4(16)MR1、12.4(16)MR2
- 12.4(17)

デバイスに Cisco製品、ログインで動作する Cisco IOSソフトウェアのバージョンを判別し、システムバナーを表示する **show version コマンドを**発行するため。 Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。 出力次の行で、イメージ名は「バージョンに」先行しているかっこと IOSリリース名の間で表示する。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVSECURITYK9-M), Version 12.4(15)T2,
   RELEASE SOFTWARE (fc7)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 17-Jan-08 23:12 by prod_rel_team
```

Cisco IOS ソフトウェア リリース指名についてのその他の情報は次のリンクで利用できます: 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

その他のCisco製品および Cisco IOS リリースは現在この脆弱性から影響を受けるために知られていません。

## 詳細

この脆弱性は SSL セッションの終了の間に引き起こされます。 ユーザ名、パスワードまたは認証のような有効な資格情報の所有物が必要となりません。 転送 プロトコルとして SSL プロトコル使用 TCP。 完全な TCP 三方ハンドシェイクの要件はこの脆弱性がスプーフィングされた IP アドレスの使用によって不正利用されること確率を減らします。

設定された SSL ベース サービスと脆弱 な Cisco IOSソフトウェアを実行するデバイスは SSL セッションを終了している間クラッシュします。

この脆弱性 Cisco バグ ID CSCsj85065 （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）ID CVE-2008-3798 は割り当てられました。

## 回避策

脆弱 な デバイスのエクスプロイトを防ぐために、SSL ベース サービスはディセーブルにされる必要があります。 ただしデバイスの定期的なメンテナンスおよびオペレーションがこのサービスに頼れば、回避策がありません。

次のコマンドは脆弱 な HTTPS サービスをディセーブルにします:

```
Router(config)#no ip http secure-server
```

次のコマンドは脆弱 な SSL VPN サービスをディセーブルにします:

```
Router(config)#no webvpn enable
```

次のコマンドは脆弱 な OSP サービスをディセーブルにします:

```
Router(config)#no settlement <n>
```

もう一つのオプションは HTTPS を使用して HTTP プロトコルへ代りに戻ることです。 この回避策のマイナス面は解決情報がネットワーク 保護されていないに送信 されることです。

不正 ホストが影響を受けたデバイスにアクセスすることを防ぐことによってこの脆弱性を軽減することは可能性のあるです。

## コントロール プレーン ポリシング（CoPP）

**コントロール プレーン ポリシング（CoPP）を**サポートする Cisco IOS ソフトウェア バージョンは管理および制御平面を目標とする不正侵入からデバイスの保護を助けるために設定することができます。 CoPP は、Cisco IOS リリース トレイン 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T で使用できます。

CoPP 次の例では、一致する ACL エントリは **policy-map ドロップする** 機能によって割り当て操作を用いるエクスプロイト パケット**拒否**操作を一致するパケットが policy-map ドロップする 機能から（示されていない）影響を受けない一方、廃棄されます:

```
Router(config)#no settlement <n>
```

**注:** CoPP 先行する例では、一致する**割り当て**操作を用いる ACL エントリは **policy-map ドロップする** 機能によってそれらのパケットの廃棄という結果にエクスプロイト パケット**拒否**操作を一致するパケットが **policy-map ドロップする** 機能から影響を受けない一方、終ります。

CoPP 機能の設定と使用方法についての詳細は、次のリンク先で確認できます。 http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html および http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html。

## Access Control List（ACL; アクセス コントロール リスト）

Access Control List（ACL）がこの脆弱性を目標とする不正侵入の軽減を助けるのに使用することができます。 ACL では、正規の送信元からのパケットのみがデバイスに到達でき、他のすべてのパケットは廃棄されるように指定できます。 次の例は、信頼できる送信元からの正規の SSL セッションを許可し、他のすべての SSL セッションを拒否する方法を示しています。

```
Router(config)#no settlement <n>
```

## 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** |
| 該当する 12.3 ベースのリリースはありません。 | | |
| **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(17a)<br>12.4(18) | 12.4(18c) |

| | | |
|---|---|---|
| 12.4JA | 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 | |
| 12.4JMC | 脆弱性なし | |
| 12.4JX | 脆弱性なし | |
| 12.4MD | 脆弱性なし | |
| 12.4MR | 12.4(19)MR | 12.4(19)MR |
| 12.4SW | 脆弱性なし | |
| 12.4T | 脆弱性なし | |
| 12.4XA | 脆弱性なし | |
| 12.4XB | 脆弱性なし | |
| 12.4XC | 脆弱性なし | |
| 12.4XD | 脆弱性なし | |
| 12.4XE | 脆弱性なし | |
| 12.4XF | 脆弱性なし | |
| 12.4XG | 脆弱性なし | |
| 12.4XJ | 脆弱性なし | |
| 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 | 脆弱性なし | |
| 12.4XQ | 脆弱性なし | |
| 12.4XT | 脆弱性なし | |
| 12.4XV | 脆弱性なし | |
| 12.4XW | 脆弱性なし | |
| 12.4XY | 脆弱性なし | |
| 12.4XZ | 脆弱性なし | |

## 不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

## 出典

## URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl

## 改訂履歴

| | | |
|---|---|---|
| リビジョン 1.1 | 2009-April-16 | 現在旧式であるように、結合されたソフトウェア テーブルへの取除かれた参照 |
| リビジョン 1.0 | 2008-September-24 | 初版リリース |

## 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。