

# Cisco IOS IPS サービス拒否の脆弱性

**High**      アドバイザリーID : cisco-sa-20080924-iosips      [CVE-2008-2739](#)  
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 : [CSCsq13348](#)

**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 侵入防御システム (IPS) 機能は SERVICE.DNS エンジンを使用するある特定の IPS シグニチャの処理で脆弱性が含まれています。この脆弱性によりルータはサービス拒否状態に終って、クラッシュするか、またはハングしますかもしれません。

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。この脆弱性に対しては回避策があります。

注: この脆弱性は CVE-2008-1447 とまったく-不正侵入の毒するキャッシュ関連していません。シスコシステムズは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns> で発見することができるその脆弱性のための Cisco Security Advisory を公開しました。

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

注: 2008 年 9 月 24 日 IOS アドバイザリーによって組み込まれる書は 12 のセキュリティ アドバイザリーが含まれています。アドバイザリーの 11 は Cisco の IOS software の脆弱性に対処し、1 つのアドバイザリーは Cisco Unified Communications Manager の脆弱性に対処します。各アドバイザリーはリリースをリストしますアドバイザリー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-ssl>
- <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-sccp)
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosfw>
- [924-l2tp](http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-l2tp)

## 該当製品

## 脆弱性のある製品

組み込みシグニチャか外部署名 ファイルを使用することを設定する場合 Cisco IOS IPS 機能で設定されるどの Cisco IOS デバイスでも脆弱、関係ないです。バージョン 4 またはバージョン 5 シグニチャを使用してデバイスはこの脆弱性から影響を受けます。

Cisco IOS IPS 機能はデフォルトで有効になりません。コマンドは **IP IPS** がインターフェイス、次次の例 Cisco IOS IPS 機能がデバイスのあらゆるインターフェイスに設定および適用されたかどうかを確認するのに使用することができることを示します:

```
Router#show ip ips interfaces
Interface Configuration
Interface FastEthernet0/0
  Inbound IPS rule is ios-ips-incoming
  Outgoing IPS rule is not set
Interface FastEthernet0/1
  Inbound IPS rule is not set
  Outgoing IPS rule is ios-ips-outgoing
Router#
```

**提示 IP IPS インターフェイスの出力は Cisco IOS IPS 機能が設定されなかったら命じまどの Cisco IOS リリースがに依存しているであるかインストールされ、デバイスで動作します。それは次の例に類似したであるかもしれません:**

```
Router#show ip ips interfaces
```

```
Router#
```

またはそれは次に類似したであるかもしれません:

```
Router#show ip ips interfaces
Interface Configuration
  IPS is not configured on any interface
Router#
```

バージョン前の Cisco IOS のどのバージョンでもソフトウェア バージョン および 修正 下記の例にリストされている脆弱です。

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。

次の例は C2500-IS-L 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 12.3(26) を実行する Cisco 製品を指定したものです:

```
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>

Router#

次の例は C1841-ADVENTERPRISEK9-M のイメージ名と Cisco IOS ソフトウェア リリース 12.4(20)T を実行する製品を示します:

```
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>

Router#

Cisco IOS リリース命名規則のその他の情報は「白書と資格を与えられる文書で見つけることができます: <http://www.cisco.com/warp/public/620/1.html> で利用可能である Cisco IOS レファレンスガイド」。

## 脆弱性を含んでいないことが確認された製品

以下のシスコ製品は確認された脆弱です:

- Intrusion detection system 機能を実行する Cisco IOS デバイス
- Intrusion detection system 機能を実行する Cisco ASA セキュリティ アプライアンス モデル
- Intrusion detection system 機能を実行する Cisco PIX 500 シリーズ セキュリティ アプライアンス
- Cisco IPS 4200 センサー
- ASA 5500 シリーズ用の Cisco AIP-SSM 適応型セキュリティ アプライアンス (ASA)
- Cisco Catalyst 6500 シリーズ Intrusion Detection System (IDSM-2) サービス モジュール

- 統合サービス ルータのための Cisco IPS Advanced Integration Module

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 IOS 侵入防御システム ( IPS ) はインライン、効果的にネットワーク攻撃の広範囲を軽減する強度の パケット インスペクション 機能です。コンポーネントは Cisco IOS 統合型の脅威制御フレームワークのおよび Cisco IOS Flexible Packet Matching ( FPM ) 補足される正確にリアルタイムの悪意のあるトラフィックを識別し、分類し、停止するか、またはブロックする知性を機能によって、Cisco IOS IPS ネットワークに与えます。Cisco IOS IPS 機能のその他の情報は [http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t8/feature/guide/gt\\_fwids.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_fwids.html) で見つけることができます。

Cisco IOS IPS 機能の概要に前、Cisco IOS は同じような機能を、Cisco IOS Intrusion detection system ( IDS ) 提供しました。Cisco IOS IDS 機能はこの脆弱性から影響を受けません。Cisco IOS IDS 機能のその他の情報は [http://www.cisco.com/en/US/docs/ios/12\\_0t/12\\_0t5/feature/guide/ios\\_ids.html](http://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/ios_ids.html) で見つけることができます。

ある特定のネットワークトラフィックは引き起こします Cisco IOS デバイスがクラッシュするか、またはハングしますかもしれない SERVICE.DNS シグニチャ エンジンの IPS シグニチャをできます。これによりネットワークトラフィックの中断という結果に終るサービス拒否を引き起こすかもしれません。この脆弱性は Cisco バグ ID [CSCsq13348](#) ( [登録ユーザのみ](#) ) で文書化されています。

この脆弱性よくある脆弱性および公開 ( CVE ) ID CVE-2008-2739 は割り当てられました。

## 回避策

回避策はデバイスで設定される各 Cisco IOS IPS ポリシーへ Access Control List ( ACL ) を追加することでポート 53/udp か 53/tcp に向かうトラフィックが Cisco IOS IPS 機能によって検査されないように構成されています。次の ACL はデバイスコンフィギュレーションに追加される必要があります:

```
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>

Router#

デバイスの Cisco IOS IPS ポリシーの各例はそれから前の ACL を参照するために修正される必要があります。どの Cisco IOS IPS ポリシーがデバイスで設定されるか判別するために、コマンド

**show running-config** を実行して下さい | IP IPS 名前を次の例含んで下さい:

```
Router#show running-config | include ip ips name  
ip ips name ios-ips-incoming  
ip ips name ios-ips-outgoing  
Router#
```

前例では、2 つの Cisco IOS IPS ポリシーはデバイスで設定されます。次の例は以前に識別される Cisco IOS IPS ポリシーの各自に ACL の付加を示したものです:

```
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#ip ips name ios-ips-incoming list 177  
Router(config)#ip ips name ios-ips-outgoing list 177  
Router(config)#end  
Router#
```

検証手順として、コマンドは ACL が Cisco IOS IPS ポリシーの各自にきちんと接続されたことを確認するために IP IPS がインターフェイス再度実行することができることを示します:

```
Router#show ip ips interfaces  
Interface Configuration  
Interface FastEthernet0/0  
Inbound IPS rule is ios-ips-incoming  
acl list 177  
Outgoing IPS rule is not set  
Interface FastEthernet0/1  
Inbound IPS rule is not set  
Outgoing IPS rule is ios-ips-outgoing  
acl list 177  
Router#
```

**注:** Cisco IOS IPS 機能の SERVICE.DNS エンジンを使用してユーザーかすべてのシグニチャをディisableにするか、または削除することは推奨される回避策ではありません。前の回避策はこの脆弱性のための唯一の Cisco 推奨回避策です。

## 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わせください。

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	
<b>Affected 12.0-Based Releases</b>	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。		
<b>Affected 12.1-Based Releases</b>	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。		
<b>Affected 12.2-Based Releases</b>	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		
<b>Affected 12.3-Based Releases</b>	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; <a href="#">first fixed in 12.4</a>	12.4(15)T7 12.4(18c)
12.3TPC	脆弱性なし	

12.3VA	脆弱性なし	
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	脆弱性あり; <a href="#">first fixed in 12.4</a>	12.4(15)T7 12.4(18c)
12.3XQ	脆弱性あり; <a href="#">first fixed in 12.4</a>	12.4(15)T7 12.4(18c)
12.3XR	脆弱性あり; <a href="#">first fixed in 12.4</a>	12.4(15)T7 12.4(18c)
12.3XS	脆弱性あり; <a href="#">first fixed in 12.4</a>	12.4(15)T7 12.4(18c)
12.3XU	脆弱性なし	
12.3XW	脆弱性なし	
12.3XX	脆弱性あり; <a href="#">first fixed in 12.4</a>	12.4(15)T7 12.4(18c)
12.3XY	脆弱性なし	
12.3XZ	脆弱性なし	
12.3YA	脆弱性あり; <a href="#">first fixed in 12.4</a>	12.4(15)T7 12.4(18c)
12.3YD	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.3YF	脆弱性なし	
12.3YG	Release prior to 12.3(8)YG7 are vulnerable , releases 12.3(8)YG7 and later are not vulnerable; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.3YH	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.3YI	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.3YJ	脆弱性なし	
12.3YK	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.3YM	12.3(14)YM13; 30-SEP-08 で利用可能	12.3(14)Y M13; 30- SEP-08 で 利用可能
12.3YQ	脆弱性なし	
12.3YS	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.3YT	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.3YU	脆弱性なし	

12.3YX	脆弱性なし	
12.3YZ	脆弱性あり; contact TAC	
12.3ZA	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
<b>Affected 12.4- Based Release s</b>	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(18b) 12.4(19a) 12.4(21)	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)M R
12.4SW	脆弱性なし	
12.4T	12.4(15)T6 12.4(20)T	12.4(15)T7
12.4XA	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.4XB	脆弱性なし	
12.4XC	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.4XD	12.4(4)XD11; 26-SEP-08 で利用可 能	12.4(4)XD 11; 26- SEP-08 で 利用可能
12.4XE	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.4XF	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.4XG	脆弱性なし	
12.4XJ	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.4XK	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
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	脆弱性あり; <a href="#">first fixed in 12.4T</a>	12.4(15)T7
12.4XV	脆弱性あり; contact TAC	
12.4XW	12.4(11)XW9	12.4(11)X W9



12.4XY	12.4(15)XY4	12.4(15)XY4
12.4XZ	12.4(15)XZ2	12.4(15)XZ2
12.4YA	12.4(20)YA1	12.4(20)YA1

## 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が不正利用に気づいていません。

この脆弱性は、お客様によって Cisco に報告されました。

## 出典

## URL

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosips>

## 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。