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

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

CVE-2008-2739

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。

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

```
! deny inspection of traffic with a destination port of 53/udp
access-list 177 deny   udp any any eq 53
! deny inspection of traffic with a destination port of 53/tcp
access-list 177 deny   tcp any any eq 53
! allow all other traffic to be inspected
access-list 177 permit ip any any
```

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**次を次の例**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無効に するか、または削除することは推奨される回避策ではないです。 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**
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	Vulnerable; 最初の修正は 12.4	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	Vulnerable; 最初の修正は 12.4	12.4(15)T7 12.4(18c)
12.3XQ	Vulnerable; 最初の修正は 12.4	12.4(15)T7 12.4(18c)
12.3XR	Vulnerable; 最初の修正は 12.4	12.4(15)T7 12.4(18c)
12.3XS	Vulnerable; 最初の修正は 12.4	12.4(15)T7 12.4(18c)
12.3XU	脆弱性なし	
12.3XW	脆弱性なし	
12.3XX	Vulnerable; 最初の修正は 12.4	12.4(15)T7 12.4(18c)
12.3XY	脆弱性なし	
12.3XZ	脆弱性なし	
12.3YA	Vulnerable; 最初の修正は 12.4	12.4(15)T7 12.4(18c)
12.3YD	Vulnerable; first fixed in 12.4T	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; first fixed in 12.4T	12.4(15)T7
12.3YH	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YI	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YJ	脆弱性なし	
12.3YK	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YM	12.3(14)YM13; 30-SEP-08 で利用可能	12.3(14)YM13; 30-SEP-08 で利用可能
12.3YQ	脆弱性なし	
12.3YS	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YT	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YU	脆弱性なし	

12.3YX	脆弱性なし	
12.3YZ	Vulnerable; contact TAC	
12.3ZA	Vulnerable; first fixed in 12.4T	12.4(15)T7
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(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)MR
12.4SW	脆弱性なし	
12.4T	12.4(15)T6 12.4(20)T	12.4(15)T7
12.4XA	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XB	脆弱性なし	
12.4XC	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XD	12.4(4)XD11; 26-SEP-08 で利用可能	12.4(4)XD11; 26-SEP-08 で利用可能
12.4XE	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XF	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XG	脆弱性なし	
12.4XJ	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XK	Vulnerable; first fixed in 12.4T	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	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XV	Vulnerable; contact TAC	
12.4XW	12.4(11)XW9	12.4(11)XW9

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 では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、お客様 によって Cisco に報告されました。

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。