Cisco IOSソフトウェア ファイアウォール アプリケーション インスペクション コントロール脆弱性

High

アドバイザリーID : cisco-sa-20080924-iosfw

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 : CSCsh12480

CVE-2008-3812

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

HTTP によって設定されるアプリケーション特有のポリシーで IOSファイアウォール アプリケーション インスペクション コントロール（AIC）のために設定される Cisco IOSソフトウェアは特定の不正 な HTTP 中継パケットを処理するときに Denial of Service（DoS/DDoS） 脆弱です。 この脆弱性の不正利用に成功した場合、影響を受けた機器では再起動が発生することがあります。

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。

この脆弱性のための軽減は利用できます。 詳細については「回避策」セクションを参照して下さい。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosfw 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-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-ipc
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sccp
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast
- 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

HTTP AIC 機能は Cisco IOS ソフトウェア リリース 12.4(9)T で導入されました。 このアドバイザリのソフトウェア テーブルは該当するリリースを識別します。

脆弱性のある製品

脆弱なバージョンを Cisco IOSソフトウェアのおよび設定される HTTP の Cisco IOS ファイアウォール AIC のために実行しているデバイスは影響を受けています。

デバイスに Cisco IOS 製品、ログインで動作するソフトウェアを判別し、システムバナーを表示するために **show version** Command Line Interface （ CLI ） 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。 出力の次の行には、カッコに囲まれたイメージ名が表示され、その後にバージョンと Cisco IOS リリース名が続きます。 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 Cisco IOSイメージ 12.4(15)T2 を実行するデバイスからの出力を示したものです:

```
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
!--- Output truncated.
```

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/web/about/security/intelligence/ios-ref.html で利用可能である Cisco IOSレファレンスガイド」。

デバイスは設定に HTTP 強度のパケット インスペクション（ 解像度 ）用のレイヤ7 クラスマップおよびレイヤ7 ポリシーマップがある、およびこれらのポリシーはあらゆるファイアウォー

ル ゾーンに適用されます場合脆弱です。 デバイスがデバイスに HTTP のための Cisco IOS ファイアウォール AIC の脆弱 な 設定を、ログイン判別し実行している、CLI コマンド **show policy-map タイプ Inspect ゾーン ペアを**発行するためかどうか **| セクション パケット点検。** 出力が**ポリシーが**含まれていれば: **http *layer7-policymap 名前は***、デバイス 脆弱です。 次の例は脆弱 な デバイスからの応答を示したものです:

```
Router#show policy-map type inspect zone-pair | section packet inspection

         Deep packet inspection
            Policy: http layer7-policymap
            1 packets, 28 bytes

Router#
```

脆弱性を含んでいないことが確認された製品

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。 12.4(9)T の前の IOS リリースはこの問題から影響を受けしません。 脆弱性が存在しない製品は下記のものを含んでいます:

- Cisco PIX
- Cisco ASA
- Cisco Firewall Services Module（FWSM）
- Cisco XR 12000 シリーズ ルータのマルチサービス ブレード（MSB）の仮想 な ファイアウォール（VFW）アプリケーション

詳細

ファイアウォールは組織のネットワーク アセットへネットワークデバイスそのコントロール アクセスです。 ファイアウォールは頻繁にネットワークに入口ポイントで置かれます。 Cisco IOSソフトウェアは特定の必要条件に従って簡単か精巧なファイアウォール ポリシーを設定することを可能にする一組のセキュリティ機能を提供します。

HTTP はネットワークで広く使われて、規格への合法性および準拠に関してまれに挑戦されるインターネット Web サービスを転送するのにポート 80 をデフォルトで使用します。 ポート 80 トラフィックがネットワークによって挑戦されないで一般的に許可されるので、多くのアプリケーション開発者はアプリケーションのトラフィックが移動するようにまた更にファイアウォールをバイパスするようにする代替転送 プロトコルとして HTTPトラフィックを活用 して います。 Cisco IOS Firewall は HTTP AIC で設定されるとき、セキュリティ ポリシー構成の範囲内で承認されない HTTP 接続を検出するためにパケット点検を行います。 それはまたポート 80 を通ってトンネリング アプリケーションであるユーザを検出する。 パケットが HTTP プロトコルに従ってない場合、廃棄されます、接続はリセットされ、syslog メッセージは適切ように、生成されます。

HTTP アプリケーション特有のポリシーで IOSファイアウォール AIC のために設定される Cisco IOSソフトウェアは特定の不正 な HTTP 中継パケットを処理するときサービス拒否状態に脆弱で

す。 この脆弱性の不正利用に成功した場合、影響を受けた機器では再起動が発生することがあります。

HTTP は TCP を実行します。 不正利用されるべきこの脆弱性に関してはどの悪意のあるトラフィックでもデバイスのリロードという結果に終るために処理される前にクライアント および サーバ間の完全な 3方向ハンドシェイクが必要となります。

HTTP アプリケーション特有のポリシーマップとの Cisco IOS Firewall AIC に関するその他の情報は /en/US/products/ps6441/products_feature_guide09186a008060f6dd.html#wp1407906 で利用できます。

この脆弱性は Cisco バグ ID CSCsh12480 （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）識別子 CVE-2008-3812 はこの脆弱性に割り当てられました。

回避策

この脆弱性に対する回避策はありません。 Help カウンターへの唯一の既知アクションはこの脆弱性影響を受けたデバイス· コンフィギュレーションの AIC HTTP 強度のパケット インスペクションを無効に することです。 深いパケット HTTP インスペクションを無効に することはファイアウォール特性がの他を設定されますソフトウェアアップグレードまで機能し続けるようにします。 他のファイアウォール特性はすべて普通実行し続けます。

AIC HTTP 強度のパケット インスペクションを無効に すること

AIC HTTP 強度のパケット インスペクションを無効に するために、**policy-map 型 Inspect** *layer4-policymap* と **policy-map 型 Inspect http** *layer7-policymap* の間でリンケージを取除いて下さい。 この例は方法に先行している現在のコンフィギュレーションを AIC HTTP 強度のパケット インスペクションを取除く示したものです:

```
!--- Existing Configuration ! parameter-map type inspect global ! class-map type inspect http
match-any layer7-classmap class-map type inspect match-any layer4-classmap match protocol http !
policy-map type inspect http layer7-policymap class type inspect http layer7-classmap allow
class class-default policy-map type inspect layer4-policymap class type inspect layer4-classmap
inspect global service-policy http layer7-policymap class class-default ! zone security inside
description ** Inside Network ** zone security outside description ** Outside Network ** zone-
pair security in2out source inside destination outside description ** Zone Pair - inside to
outside ** service-policy type inspect layer4-policymap
```

疑わしいゾーン ペアからサービス ポリシーを取除いて下さい:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#zone-pair security in2out source inside destination outside
Router(config-sec-zone-pair)#no service-policy type inspect layer4-policymap Router(config-sec-
zone-pair)#exit
```

policy-map 型 Inspect *layer4-policymap* と **policy-map 型 Inspect http** *layer7-policymap* の間でリンケージを取除いて下さい:

```
Router(config)#policy-map type inspect layer4-policymap Router(config-pmap)#class type inspect
layer4-classmap Router(config-pmap-c)#no service-policy http layer7-policymap Router(config-
pmap-c)#exit
Router(config-pmap)#exit
```

疑わしいゾーン ペアにサービス ポリシーを再適用して下さい:

```
Router(config)#zone-pair security in2out source inside destination outside
Router(config-sec-zone-pair)#service-policy type inspect layer4-policymap Router(config-sec-
zone-pair)#exit
```

必要とされなくて、なぜならが設定の完璧さ **policy-map 型 Inspect http** *layer7-policymap* および **class-map 型 Inspect http match-any** *layer7-classmap* は取除かれるために推奨されます。

```
Router(config)#no policy-map type inspect http layer7-policymap Router(config)#no class-map type
inspect http match-any layer7-classmap Router(config)#exit
Router#
```

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	脆弱性なし	
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	脆弱性なし	
12.4SW	脆弱性なし	
12.4T	12.4(9)T 以前のリリースは脆弱ではないです。 で固定される第 1: 12.4(9)T7 12.4(11)T4 12.4(15)T	12.4(15)T7
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	Vulnerable; first fixed in 12.4T	12.4(15)T7

12.4XF	脆弱性なし	
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	脆弱性なし	
12.4XV	Vulnerable; contact TAC	
12.4XW	12.4(11)XW1	12.4(11)XW9
12.4XY	脆弱性なし	
12.4XZ	脆弱性なし	
12.4YA	脆弱性なし	

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 Cisco 内部テストによって発見されました。

URL

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

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。