Cisco IOSソフトウェア ゾーン ベースのポリシー ファイアウォール脆弱性

High

アドバイザリーID : cisco-sa-20090923-ios-fw

初公開日 : 2009-09-23 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 : CSCsr18691

CVE-2009-2867

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 ゾーン ベースのポリシー ファイアウォール セッション開始プロトコル（SIP）インスペクションで設定される Cisco IOS® デバイスは仕様 SIP 中継パケットを処理するときサービス拒否（DoS）不正侵入に脆弱です。 脆弱性の不正利用は影響を受けたデバイスのリロードという結果に終る可能性があります。

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。

この脆弱性を軽減する回避策は利用できます。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ios-fw で掲示されます

注: 2009 年 9 月 23 日の IOS アドバイザリ バンドル公開には 11 件の Security Advisory が含まれています。 10 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、 1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。 各アドバイザリには、そのアドバイザリ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。

"Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" の個々の公開リンクは次のリンク内に掲載されています:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

該当製品

この脆弱性は Cisco IOS ソフトウェア リリースの限られた数に影響を与えます。 該当するリリースの詳細についてはこのアドバイザリの「ソフトウェア バージョン および 修正」セクションを参照して下さい。

Cisco IOS ゾーン ベースのポリシー ファイアウォール SIP インスペクション（UDP ポート 5060、TCP ポート 5060、およびで 5061）設定されるデバイスだけ脆弱です。 SIP （コンテキストベース アクセス コントロール（CBAC））のためのレガシー Cisco IOS Firewall サポートで設定される Cisco IOSデバイス 脆弱 でであってはなりません。

脆弱性のある製品

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "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 ソフトウエア リリース名が表示されます。 他のシスコ デバイスでは、**show version** コマンドが存在しなかったり、別の出力が表示されたりします。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
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 Â©) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

次の例は C1841-ADVENTERPRISEK9-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, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright Â©) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Cisco IOS ソフトウエ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

デバイスは設定に設定されるレイヤ3 かレイヤ7 SIP アプリケーション特有のポリシーがある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あり。 デバ

イスがデバイスに脆弱 な 設定を、ログイン判別し実行している、Command Line Interface（CLI）コマンド **show policy-map 型 Inspect ゾーン ペアを**発行するためかどうか **| atch を含んで下さい: access|プロトコルーロ。** 出力が「**ー致が**含まれていれば: **プロトコルーロは**」、デバイス 脆弱です。 出力が**ー致が**含まれていれば: ***グループ番号は***、それからデバイス 脆弱 その時だけ、参照されたアクセス リスト割り当て SIP プロトコル（UDP ポート 5060、TCP 5060 および 5061）です。 次の例は Cisco IOS ゾーン ベースのポリシー ファイアウォール SIP インスペクションで設定される脆弱 な デバイスを示したものです:

```
Router#show policy-map type inspect zone-pair | include atch: access|protocol sip
      Match: protocol sip
Router#
```

次の例は応用アクセス リストを通って SIP インスペクションで設定される脆弱 な デバイスを示したものです:

```
Router#show policy-map type inspect zone-pair | include atch: access|protocol sip
      Match: access-group 102
Router#
Router#show access-list 102
Extended IP access list 102
    10 permit udp any any eq 5060
    20 permit tcp any any eq 5060
    30 permit tcp any any eq 5061
Router#
```

SIP インスペクション用に設定されないし、この設定をサポートしないデバイスはブランク 行かエラーメッセージを返します。 以下は Cisco IOS Firewall をサポートするで有効に なる SIP インスペクションがありませんデバイスの例:

```
Router#show policy-map type inspect zone-pair | include atch: access|protocol sip
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。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 500 シリーズ ファイアウォール
- Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Catalyst 6500 スイッチ用の Firewall Services Module（FWSM）および 7600 シリーズ ルータ
- 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
- Cisco ACE アプリケーション コントロール エンジン モジュール
- Cisco IOS ゾーン ベースのポリシー ファイアウォール SIP インスペクションで設定されない Cisco IOSデバイス。
- SIP（CBAC）のためのレガシー Cisco IOS Firewall サポートで設定される Cisco IOSデバ

イス
- Cisco IOS XE ソフトウェア
- Cisco IOS XR ソフトウェア

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。

Cisco IOS Firewall の SIP インスペクションは基本 SIP Inspect 機能（SIP パケット点検およびピンホール開始）、またプロトコル準拠およびアプリケーションセキュリティ提供します。

Cisco IOS ゾーン ベースのポリシー ファイアウォール SIP インスペクションで設定される Cisco IOSソフトウェアは仕様 SIP 中継パケットを処理するとき DoS攻撃に脆弱です。 この脆弱性の不正利用は影響を受けたデバイスのリロードという結果に終ります。

Cisco IOS ゾーン ベースのポリシー ファイアウォール SIP インスペクションは Cisco IOS ソフトウェア バージョン 12.4(15)XZ および 12.4(20)T で最初にもたらされました。

ip inspect 名前[inspection_name]ー口を通って SIP インスペクション用の Cisco IOS Firewall CBAC サポートは脆弱ではないです。 SIP インスペクション用の Cisco IOS Firewall CBAC サポートに関するその他の情報は次のリンクで文書「SIP のためのファイアウォール サポート」で利用できます:
http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_fwall_sip_supp.html

Cisco IOS ゾーン ベースのポリシー ファイアウォール SIP インスペクションに関するその他の情報は文書で利用できます「Cisco IOS Firewall: SIP の機能強化： 次のリンクの ALG および AIC」: http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html

この脆弱性は次の Cisco バグ ID で文書化されています: **CSCsr18691**（登録ユーザのみ）およびよくある脆弱性および公開（CVE）識別子 CVE-2009-2867 は割り当てられました。

回避策

この脆弱性のための唯一の回避策は Cisco IOS 影響を受けたデバイス· コンフィギュレーションのゾーン ベースのポリシー ファイアウォール SIP インスペクションをディセーブルにすることです。 SIP インスペクションをディセーブル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。 SIP インスペクションをディセーブルにすることは SIP インスペクション ファイアウォールの実装によって変わります。

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**
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	
12.4GC	脆弱性なし	

12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JDC	脆弱性なし	
12.4JDD	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	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MDA	脆弱性なし	
12.4MR	脆弱性なし	
12.4SW	脆弱性なし	
12.4T	12.4(20)T 以前のリリースは脆弱ではないです; 12.4(20)T2 12.4(22)T1 12.4(24)T	12.4(20)T4 12.4(22)T3 12.4(24)T2 ; 23-OCT-2009 で利用可能
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	
12.4XR	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	脆弱性あり; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2 ; 23-OCT-2009 で利用可能

12.4YA	脆弱性あり; first fixed in 12.4T	12.4(22)T3 12.4(24)T2 ; 23-OCT-2009 で利用可能
12.4YB	12.4(22)YB4	12.4(22)YB4 12.4(22)YB5; 19-OCT-2009 で利用可能
12.4YD	脆弱性なし	
12.4YE	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。

この脆弱性は Cisco 内部テストによって検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ios-fw

改訂履歴

リビジョン 1.0	2009-September-23	初版リリース

利用規約