Cisco IOSソフトウェアのSession Initiation ProtocolにおけるDoS脆弱性

アドバイザリーID : cisco-sa-20100324-sip
初公開日 : 2010-03-24 16:00
最終更新日 : 2012-09-21 19:11
バージョン 1.1 : Final
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID : CSCsz89904 CSCsz48680 CSCtb93416

CVE-2010-0580
CVE-2010-0581
CVE-2010-0579

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®ソフトウェアのSession Initiation Protocol(SIP)実装には複数の脆弱性があり、認証されていないリモートの攻撃者がSIP操作を有効にしたときに該当デバイスのリロードを引き起こす可能性があります。リモートコード実行も可能です。

シスコはこれら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ています。SIPを実行する必要があるデバイスについては回避策はありません。ただし、脆弱性の発現を抑える対応策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-sip で公開されています。

注：2010年3月24日のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開には7件のSecurity Advisoryが含まれています。すべてのアドバイザリで Cisco IOS ソフトウェアの脆弱性が取り上げられています。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。2010 年 3 月 24 日またはそれ以前に公開されたすべての Cisco IOS ソフトウェアの脆弱性に対応したリリースについては、次の URL にある表を参照してください。

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-bundle

個々の公開リンクは、次のリンクの「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar10.html

該当製品

これらの脆弱性が該当するのは、SIP音声サービスが有効になっているCisco IOSソフトウェアを実行しているデバイスだけです。

脆弱性のある製品

該当するバージョンのCisco IOSソフトウェアが稼働し、SIPメッセージを処理するように設定されているシスコデバイスが影響を受けます。

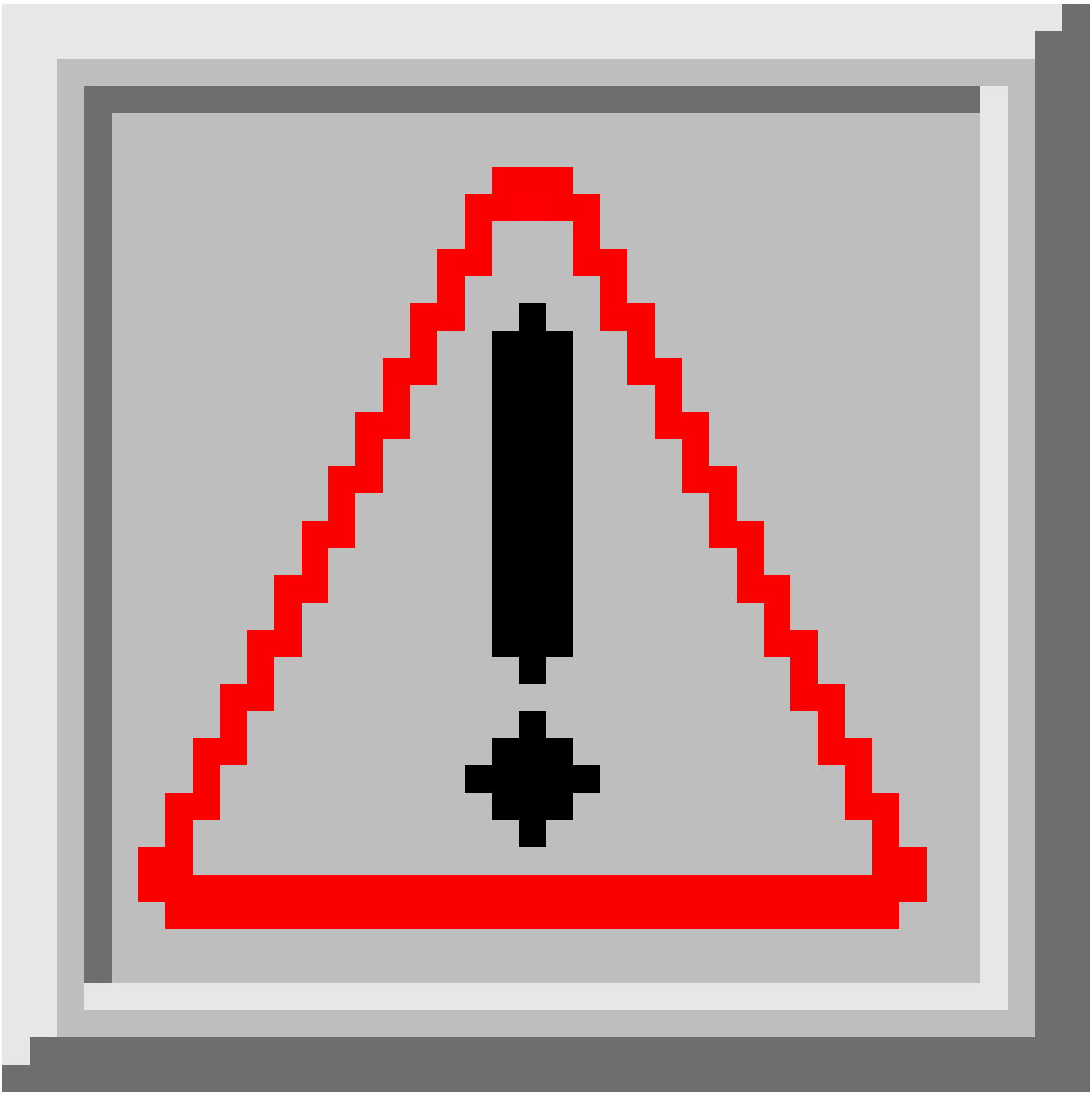
Cisco IOSソフトウェアの最近のバージョンでは、デフォルトではSIPメッセージは処理されません。dial-peer voiceコマンドを発行してダイヤルピアを作成すると、SIPプロセスが開始され、Cisco IOSデバイスでSIPメッセージが処理されます。また、ePhoneなどのCisco Unified Communications Manager Expressの一部の機能を設定すると、SIPプロセスが自動的に開始されるため、デバイスはSIPメッセージの処理を開始します。該当する設定の例を次に示します。

```
dial-peer voice <Voice dial-peer tag> voip
 ...
!
```

Cisco IOSデバイスの設定でdial-peerコマンドを検査してデバイスがSIPメッセージを処理できるようにするだけでなく、管理者はshow processesコマンドを使用することもできます| include SIPコマンドを実行して、Cisco IOSソフトウェアがSIPメッセージを処理するプロセスを実行しているかどうかを確認します。次の例では、プロセスCCSIP_UDP_SOCKETまたはCCSIP_TCP_SOCKETが存在するため、Cisco IOSデバイスがSIPメッセージを処理することが示されています。

<#root>

```
Router#
show processes | include SIP
 149 Mwe 40F48254            4          1    400023108/24000  0 CCSIP_UDP_SOCKET
 150 Mwe 40F48034            4          1    400023388/24000  0 CCSIP_TCP_SOCKET
```



警告：Cisco IOSソフトウェアを実行しているデバイスがSIPメッセージの処理を開始する方法は複数あるため、show processes | include SIPコマンドを使用すると、特定の設定コマンドの存在に依存する代わりに、デバイスがSIPメッセージを処理しているかどうかを確認できます。

Cisco Unified Border Elementイメージもこれらの脆弱性の影響を受けます。

注：Cisco Unified Border Element機能（旧称Cisco Multiservice IP-to-IP Gateway）は、Ciscoマルチサービスゲートウェイプラットフォームで動作する特別なCisco IOSソフトウェアイメージです。課金、セキュリティ、コールアドミッション制御、Quality of Service(QoS)、およびシグナリングインターワーキングのためのネットワーク間インターフェイスポイントを提供します。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログ

インして show version コマンドを使って、システム バナーを表示します。"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:

<#root>

```
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
```

次の例は、インストールされたイメージ名が C1841-ADVENTERPRISEK9-M で、Cisco IOS ソフトウェア リリース 12.4(20)T を実行しているシスコ製品を示しています。

<#root>

```
Router#

show version

Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc
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
```

Cisco IOSソフトウェアリリースの命名規則の追加情報は、次のリンクの「White Paper: Cisco IOS Reference Guide」で確認できます。http://www.cisco.com/warp/public/620/1.html。

脆弱性を含んでいないことが確認された製品

Cisco IOS NATおよびCisco IOSソフトウェアのファイアウォール機能によって使用されるSIPアプリケーションレイヤゲートウェイ(ALG)は、これらの脆弱性の影響を受けません。

Cisco IOS XEソフトウェアおよびCisco IOS XRソフトウェアは、これらの脆弱性の影響を受けません。

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

SIPは、インターネットなどのIPネットワークを介した音声およびビデオコールの管理に使用される一般的なシグナリングプロトコルです。SIPは、コールのセットアップと終了のすべての側面を処理する役割を担います。音声とビデオは、SIPで処理される最も一般的なセッションタイプですが、このプロトコルには、コールのセットアップと終了を必要とする他のアプリケーションに対応できる柔軟性があります。SIPコールシグナリングでは、基本のトランスポートプロトコルとしてUDP（ポート5060）、TCP（ポート5060）、またはTLS（TCPポート5061）を使用できます。

Cisco IOSソフトウェアのSIP実装には3つの脆弱性があり、リモート攻撃者がデバイスのリロードを引き起こしたり、任意のコードを実行したりする可能性があります。これらの脆弱性は、Cisco IOSソフトウェアを実行しているデバイスが不正なSIPメッセージを処理すると引き起こされます。

SIPがTCPトランスポート上で実行されている場合、これらの脆弱性を不正利用するにはTCP 3ウェイハンドシェイクが必要です。

これらの脆弱性は、Cisco Bug ID CSCsz48680（登録ユーザ専用）、CSCsz89904(登録ユーザ専用)、およびCSCtb93416(登録ユーザ専用)で対処され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2010-0580、CVE-2010-0581およびCVE-2010が0が0割6になっていますそれぞれ0579です。

回避策

該当するCisco IOSデバイスでVoIPサービス用にSIPが必要な場合、SIPを無効にすることはできません。また、回避策はありません。脆弱性の発現を制限するために、緩和テクニックを適用することを推奨します。緩和策とは、正当なデバイスだけが該当するデバイスに接続できるようにすることです。効果を高めるには、この緩和策をネットワークエッジのアンチスプーフィングと組み合わせて使用する必要があります。SIPはトランスポートプロトコルとしてUDPを使用できるため、このアクションは必須です。

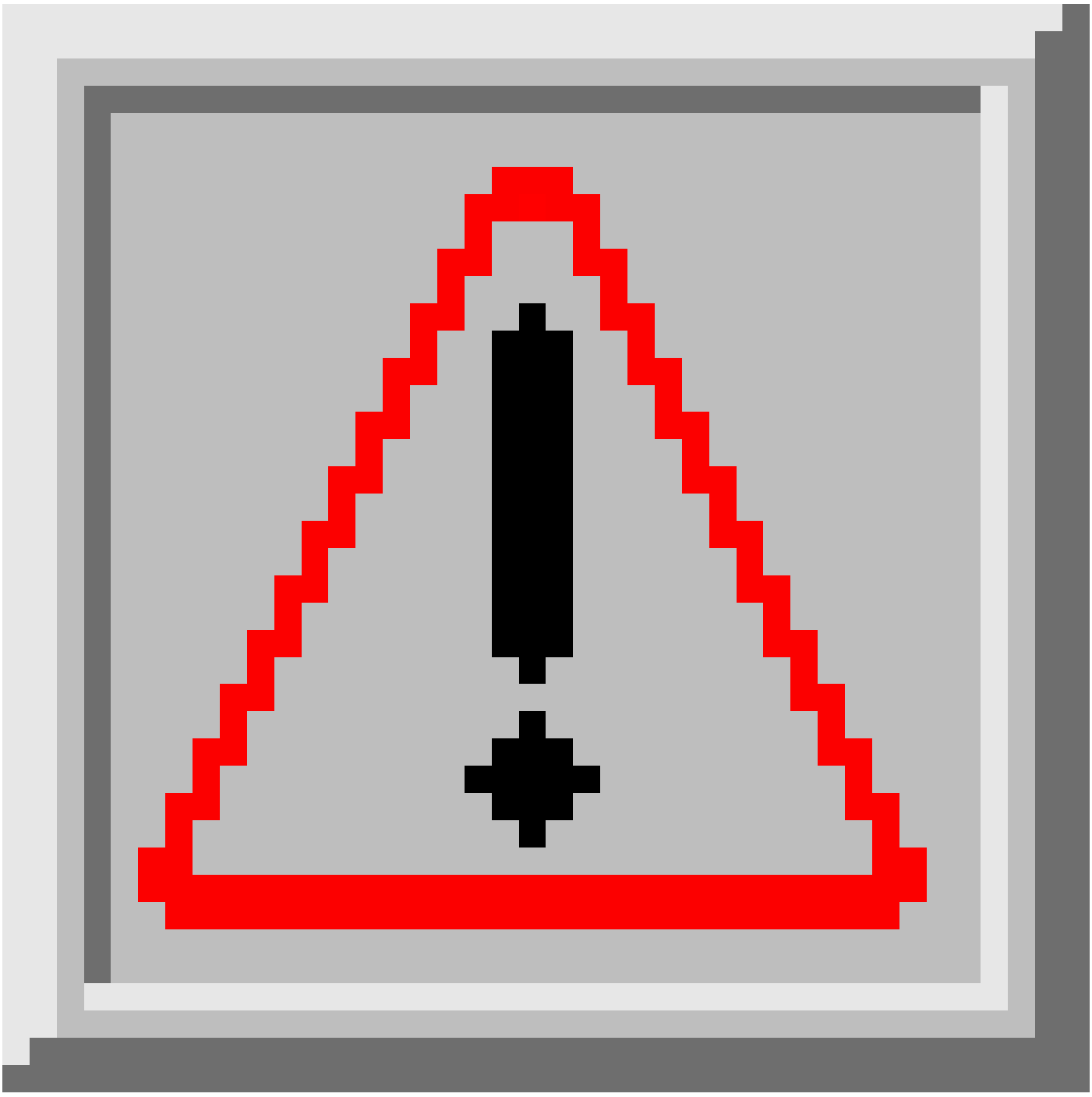
ネットワーク内のCiscoデバイスに適用可能な他の対応策は、次のURLにある付属ドキュメント『Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager Express and Cisco IOS Software H.323 and Session Initiation Protocol Denial of Service Vulnerabilities』に記載されています。https://sec.cloudapps.cisco.com/security/

center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100324-voice

SIPリスニングポートの無効化

SIPを有効にする必要がないデバイスの場合、最も簡単で効果的な回避策は、デバイスのSIP処理を無効にすることです。Cisco IOSソフトウェアの一部のバージョンでは、管理者は次のコマンドを使用してSIPを無効にすることができます。

```
sip-ua
 no transport udp
 no transport tcp
 no transport tcp tls
```



警告：Media Gateway Control Protocol(MGCP)またはH.323コールを処理しているデバイスにこの回避策を適用すると、アクティブコールの処理中にデバイスでSIP処理が停止されません。このような状況では、この回避策は、アクティブコールを一時的に停止できるメンテナンスウィンドウ中に実装する必要があります。

show udp connections、show tcp brief all、およびshow processes | include SIPコマンドを使用すると、この回避策を適用した後でSIP UDPポートとTCPポートが閉じていることを確認できます。

使用しているCisco IOSソフトウェアのバージョンによっては、show ip socketsコマンドの出力にSIPポートが開いていることが示される場合がありますが、それらにトラフィックを送信するとSIPプロセスが次のメッセージを表示します。

```
*Feb  2 11:36:47.691: sip_udp_sock_process_read: SIP UDP Listener is DISABLED
```

コントロール プレーン ポリシング

SIPサービスを提供する必要があるデバイスでは、コントロールプレーンポリシング(CoPP)を使用して、信頼できない送信元からデバイスへのSIPトラフィックをブロックすることができます。CoPP機能は、Cisco IOSリリース12.0S、12.2SX、12.2S、12.3T、12.4、および12.4Tでサポートされています。デバイスに CoPP を設定して、管理プレーンとコントロール プレーンを保護し、既存のセキュリティ ポリシーおよび設定に従って、インフラストラクチャのデバイスに送信される承認されたトラフィックだけを明示的に許可することで、インフラストラクチャへの直接攻撃のリスクと効果を最小限に抑えることができます。次の例は、特定のネットワーク設定に適用できます。

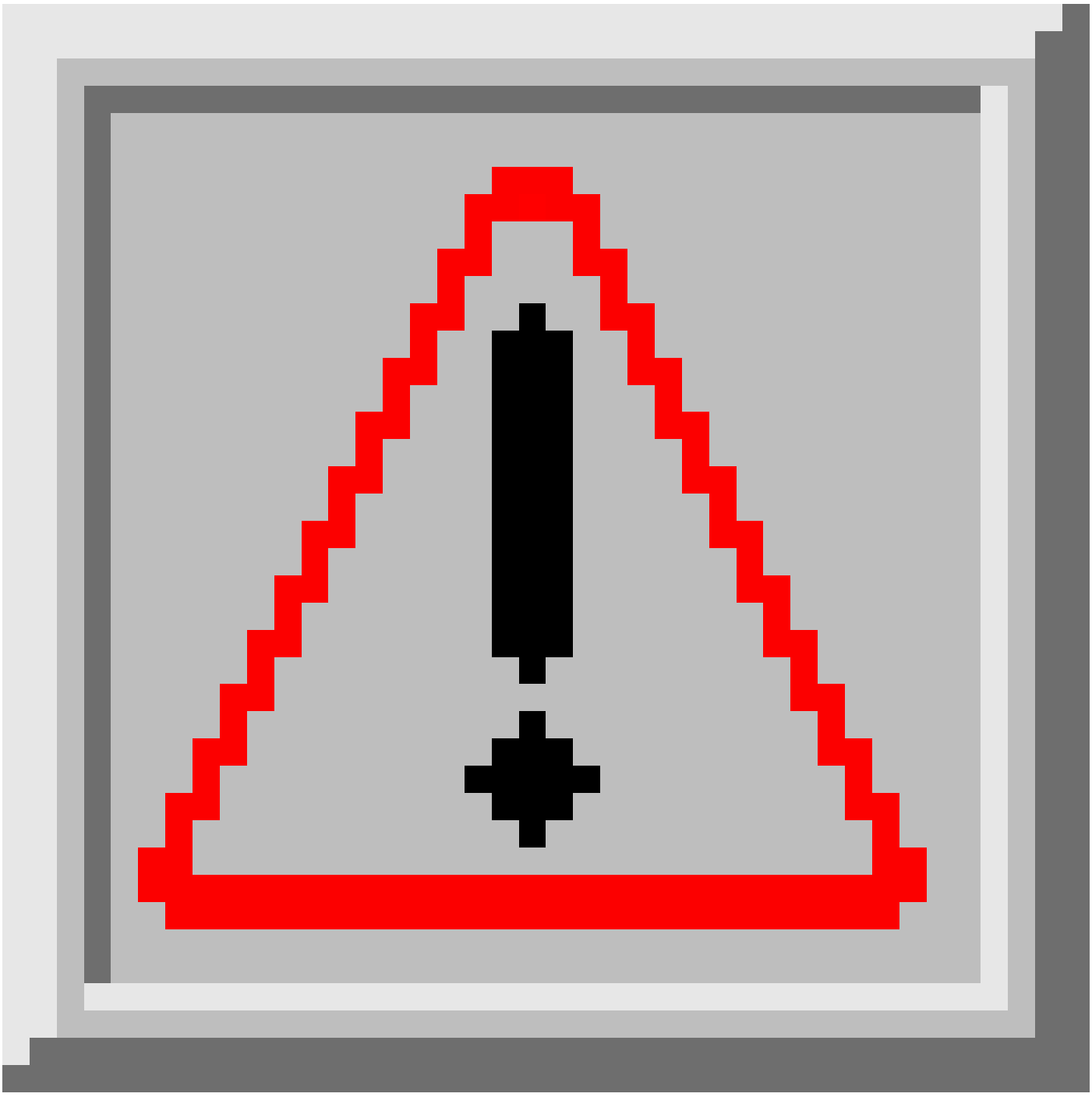
```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature.) If the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.
access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061


!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.
class-map match-all drop-sip-class
  match access-group 100


!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
policy-map control-plane-policy
 class drop-sip-class
  drop


!-- Apply the Policy-Map to the Control-Plane of the
!-- device.
control-plane
```

```
service-policy input control-plane-policy
```



警告： SIPではトランスポートプロトコルとしてUDPを使用できるため、送信者のIPアドレスを簡単にスプーフィングすることが可能です。これにより、信頼できるIPアドレスからこれらのポートへの通信を許可するアクセスコントロールリスト(ACL)を無効にできる可能性があります。

上記のCoPPの例では、access control entries（ACE；アクセスコントロールエントリ）の潜在的な悪用パケットに「permit」アクションが一致する場合、これらのパケットはポリシーマップの「drop」機能によって廃棄されますが、「deny」アクション（非表示）に一致するパケットは、ポリシーマップのdrop機能の影響を受けません。CoPP 機能の設定と使用に関する詳細は、http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html および http://www.cisco.com/en/U

S/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

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存在する場合、その修正を含む最初のリリース（および該当する場合は、それぞれで利用可能になる予定日）が表の「このアドバイザリの最初の修正済みリリース」列に記載されます。「2010年3月24日のバンドル公開に含まれるすべてのアドバイザリの最初の修正リリース」列は、このCisco IOSセキュリティアドバイザリバンドル公開で公開されているすべての脆弱性に対する修正を含む最初のリリースを示しています。可能な場合は、利用可能な最新のリリースにアップグレードすることをお勧めします。

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	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
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	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
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	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
影響を受ける 12.2 ベースのリリースはありません。		
Affected 12.3-Based Releases	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
12.3	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3B	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3BC	脆弱性なし	脆弱性あり（最初の修正は12.2SCB）
12.3BW	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3EU	脆弱性なし	脆弱性なし
12.3JA	脆弱性なし	12.3(11)JA5 より前の

		リリースには脆弱性があり、12.3(11)JA5 以降のリリースには脆弱性はありません。
12.3JEA	脆弱性なし	12.3(8)JEA4 より前のリリースには脆弱性があり、12.3(8)JEA4 以降のリリースには脆弱性はありません。
12.3JEB	脆弱性なし	12.3(8)JEB2 より前のリリースには脆弱性があり、12.3(8)JEB2 以降のリリースには脆弱性はありません。
12.3JEC	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.3JED	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.3JK	12.3(2)JK3 までのリリースには脆弱性はありません。 リリース 12.3(8)JK1以降には	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。

	脆弱性はありません。最初の修正は12.4です。	
12.3JL	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.3JX	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.3T	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。12.3(4)T11までのリリースには脆弱性はありません。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3TPC	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.3VA	脆弱性なし	脆弱性なし
12.3XA	脆弱性なし	脆弱性あり。15.0Mの

		任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XB	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.3XC	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XD	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XE	脆弱性なし	脆弱性あり(最初の修正は12.4) 脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XF	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください

12.3XG	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XI	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	12.3(7)XI11 より前のリリースには脆弱性があり、12.3(7)XI11 以降のリリースには脆弱性はありません。
12.3XJ	脆弱性あり。 12.4XNの任意のリリースに移行	脆弱性あり(最初の修正は12.4XR)
12.3XK	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XL	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XQ	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XR	脆弱性あり。15.0Mの任意のリリースまた	脆弱性あり。15.0Mの任意のリリースまたは

	は修正済み12.4リリースに移行してください。	修正済み12.4リリースに移行してください。
12.3XS	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XU	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。 12.3(8)XU1までのリリースには脆弱性はありません。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XW	脆弱性あり。 12.4XNの任意のリリースに移行	脆弱性あり(最初の修正は12.4XR)
12.3XX	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XY	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3XZ	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは

		修正済み12.4リリースに移行してください。
12.3YA	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YD	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YF	脆弱性あり。12.4XNの任意のリリースに移行	脆弱性あり(最初の修正は12.4XR)
12.3YG	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YH	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YI	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YJ	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリース

		に移行してください。
12.3YK	12.3(11)YK3より前のリリースには脆弱性があり、12.3(11)YK3以降のリリースには脆弱性はありません。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YM	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YQ	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YS	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。 12.3(11)YS1までのリリースには脆弱性はありません。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YT	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。

12.3YU	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.3YX	脆弱性あり。 12.4XNの任意のリリースに移行	脆弱性あり(最初の修正は12.4XR)
12.3YZ	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.3ZA	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
Affected 12.4-Based Releases	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
12.4	12.4(25c) 15.0(1)M1 15.0(1)M2（2010年3月26日に入手可能）	12.4(25c) 15.0(1)M1

12.4GC	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JA	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JDA	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JDC	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JDD	脆弱性なし	12.4(10b)JDD1
12.4JHA	脆弱性なし	脆弱性なし
12.4JK	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従

		って、サポート組織にお問い合わせください
12.4JL	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JMA	脆弱性なし	12.4(3g)JMA2 より前のリリースには脆弱性があり、 12.4(3g)JMA2 以降のリリースには脆弱性はありません。
12.4JMB	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JX	脆弱性なし	脆弱性あり(最初の修正は12.4JA)
12.4MD	12.4(24)MD 12.4(22)MDより前のリリースには脆弱性はありません。 12.4(22)MD1より後のリリースには脆弱性はありません。	12.4(24)MD
12.4MDA	12.4(22)MDA2	12.4(22)MDA2

12.4MR	12.4(9)MRより前のリリースには脆弱性があり、12.4(9)MR以降のリリースには脆弱性はありません	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4SW	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4T	12.4(22)T3 12.4(24)T2	12.4(15)T12 12.4(20)T5 12.4(24)T3（2010年3月26日に入手可能） 12.4(22)T4
12.4XA	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XB	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XC	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。

12.4XD	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XE	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XF	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XG	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XJ	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XK	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XL	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織に

		お問い合わせください
12.4XM	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XN	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XP	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XQ	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XR	12.4(22)XR3; 脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。 12.4(15)XR8までのリリースには脆弱性はありません。	12.4(22)XR3

12.4XT	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XV	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XW	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XY	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XZ	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4YA	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4YB	12.4(22)YB5	脆弱性あり。このアドバイザリの「修正済み

		ソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4YD	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4YE	12.4(22)YE2 12.4(24)YE	12.4(22)YE2 12.4(24)YE
12.4YG	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
影響を受ける 15.0 ベースのリリース	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
影響を受ける 15.0 ベースのリリースはありません。		
影響を受ける 15.1 ベースのリリース	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正

		リリース
影響を受ける 15.1 ベースのリリースはありません。		

Cisco IOS XE ソフトウェア

IOS XE リリース	First Fixed Release（修正された最初のリリース）
2.1.x	脆弱性なし
2.2.x	脆弱性なし
2.3.x	脆弱性なし
2.4.x	脆弱性なし
2.5.x	脆弱性なし
2.6.x	脆弱性なし

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

CSCsz48680 (登録ユーザ専用)で対処されている脆弱性は、お客様からのサービスリクエストの解決中に発見されました。

CSCtb93416 (登録ユーザのみ)およびCSCsz89904(登録ユーザのみ)で対処される脆弱性は、シスコの社内テストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-sip

改訂履歴

リビジョン 1.1	2010/3-29	12.4Tの最初の修正済みリリースを更新
リビジョン 1.0	2010 年 3 月 24 日	初版リリース

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。