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

High

アドバイザリーID : cisco-sa-20090325-sip CVE-2009-0636
初公開日 : 2009-03-25 16:00
バージョン 1.4 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCsu11522

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)の実装には脆弱性が存在し、リモートから悪用されてCisco IOSデバイスのリロードを引き起こす可能性があります。

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ています。Cisco IOSデバイスでVoIPサービス用にSIPを実行する必要がない場合、SIPを無効にする以外に、この脆弱性を軽減する回避策はありません。ただし、脆弱性の発現を制限するために、緩和テクニックを利用できます。

このアドバイザリは、次のリンクに掲載されます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip。

注：2009年3月25日のCisco IOSセキュリティアドバイザリバンドル公開には8件のSecurity Advisoryが含まれています。これらのアドバイザリはすべて、Cisco IOSソフトウェアの脆弱性に対処するものです。各アドバイザリには、そのアドバイザリに記載された脆弱性を修正するリリースが記載されています。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCPのDoS脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ctcp

- Cisco IOSソフトウェアの複数の機能におけるIPソケットの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

20090325-ip

- Cisco IOSソフトウェアモバイルIPおよびモバイルIPv6の脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip

- Cisco IOSソフトウェアのSecure Copyにおける権限昇格の脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp

- Cisco IOSソフトウェアのSession Initiation ProtocolにおけるDoS脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

- Cisco IOSソフトウェアの複数の機能における巧妙に細工されたTCPシーケンスの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- Cisco IOSソフトウェアの複数機能における巧妙に細工されたUDPパケットの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

- Cisco IOSソフトウェアのWebVPNおよびSSLVPNの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

この脆弱性の影響を受けるのは、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Cisco IOSソフトウェアバージョンを実行し、SIPメッセージを処理するシスコデバイ

スは、この脆弱性の影響を受けます。この脆弱性の唯一の要件は、Cisco IOSデバイスが設定されたVoIP機能の一部としてSIPメッセージを処理することです。これは、NATおよびファイアウォール機能セットの一部としてのSIPメッセージの処理には適用されないことに注意してください。

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。コマンドdial-peer voiceを使用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メッセージの処理が開始されます。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
 ...
!
```

注：Cisco IOSソフトウェアの古いバージョンは、Cisco IOSソフトウェアがSIP動作を設定せずにSIPメッセージを処理する原因となったバグの影響を受けました。Cisco Bug ID CSCsb25337 (登録ユーザ専用)の詳細については、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070131-sipを参照してください。

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およびCCSIP_TCP_SOCKETが存在することから、Cisco IOSデバイスがSIPメッセージを処理していることがわかります。

```
Router#show processes | include SIP
 147 Mwe 40F46DF4           12          2    600023468/24000  0 CCSIP_SPI_CONTRO
 148 Mwe 40F21244            0          1       0 5524/6000   0 CCSIP_DNS
 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。

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:

```
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。

```
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ソフトウェアを実行しているシスコデバイスは影響を受けません。

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、サービス拒否(DoS)の脆弱性が存在します。この脆弱性は、特定の有効なSIPメッセージを処理することによって引き起こされます。

この脆弱性は、Cisco Bug ID CSCsu11522 (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-0636が割り当てられています。

注：このCisco IOSアドバイザリバンドルの一部であるCisco IOS Software Multiple Features IP Sockets VulnerabilityおよびCisco IOS Software Multiple Features Crafted UDP Packet Vulnerabilityに記載されている脆弱性もSIPの動作に影響を与える可能性があります。

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。したがって、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。緩和策は、正当なデバイスだけがルータ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、次のリンクにある付属ドキュメント『Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS SIP and Crafted UDP Vulnerabilities』で参照できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090325-sip-and-udp。

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これを実行できます。

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

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。

この回避策を適用した後は、このアドバイザリの「該当製品」セクションで説明されているshowコマンドを使用して、Cisco IOSデバイスがSIPメッセージを処理していないことを確認することを推奨します。

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、ネットワークに適用できます。

```
!-- 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 drop-sip-traffic
 class drop-sip-class
  drop

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

control-plane
 service-policy input drop-sip-traffic
```

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Access Control List（ACL；アクセスコントロールリスト）を無効にすることができます。

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/US/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。

注：この修正済みソフトウェアの表では、CSCsu11522 に加えて、SIPの動作への影響により、『Cisco Security Advisory: Crafted UDP Packet Affects Multiple Cisco IOS Features』(https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp)で説明されているCisco Bug CSCsk64158 で追跡される脆弱性も考慮されています。 この表では、「Cisco Security Advisory: Cisco IOS IP Sockets Vulnerability Affecting Multiple Cisco IOS Features」によって公開された脆弱性は考慮されていません。この脆弱性はSIP over TLSに影響を与える可能性があります。

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
12.0	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0DA	脆弱性あり(最初の修正は12.2DA)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0DB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0DC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）

12.0S	12.0(32)S12	12.0(32)S12
12.0SC	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0SL	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0SP	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0ST	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0SX	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0SY	12.0(32)SY8	12.0(32)SY8
12.0SZ	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0T	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0W	脆弱性あり。TACに連絡	
12.0WC	脆弱性あり。TACに連絡	

12.0WT	脆弱性なし	
12.0XA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XF	脆弱性なし	
12.0XG	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月

		5日に入手可能）
12.0XI	12.0(4)XI2より前のリリースには脆弱性があり、12.0(4)XI2以降のリリースには脆弱性はありません。最初の修正は12.4です。	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XJ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XK	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XL	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XM	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XN	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XQ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）

12.0XR	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XS	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XT	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XV	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
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
12.1	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1AA	脆弱性あり。TACに連絡	
12.1AX	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.1AY	脆弱性あり(最初の修正	12.1(22)EA13

	は12.1EA)	12.2(44)SE6
12.1AZ	脆弱性あり(最初の修正は12.1EA)	12.1(22)EA13 12.2(44)SE6
12.1CX	脆弱性あり。TACに連絡	
12.1DA	脆弱性あり。TACに連絡	
12.1DB	脆弱性あり。TACに連絡	
12.1DC	脆弱性あり。TACに連絡	
12.1E	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.1EA	12.1(22)EA13	12.1(22)EA13
12.1EB	脆弱性あり。TACに連絡	
12.1EC	脆弱性あり(最初の修正は12.3BC)	12.2(33)SCB1 12.3(23)BC6
12.1EO	脆弱性あり。TACに連絡	

12.1EU	脆弱性あり(最初の修正は12.2SG)	12.2(31)SGA9
12.1EV	脆弱性あり。TACに連絡	
12.1EW	脆弱性あり、12.2SGAに移行	12.2(31)SGA9
12.1EX	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1EY	脆弱性あり。TACに連絡	
12.1EZ	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.1GA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1GB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1T	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XA	脆弱性あり(最初の修正	12.4(18e)

	は12.4)	12.4(23a)（2009年6月5日に入手可能）
12.1XB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XF	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XG	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）

12.1XI	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XJ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XL	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XM	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XP	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XQ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XR	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XS	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月

		5日に入手可能）
12.1XT	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XU	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XV	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XW	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XX	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XY	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XZ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）

12.1YA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YE	12.1(5)YE6より前のリリースには脆弱性があり、12.1(5)YE6以降のリリースには脆弱性はありません。最初の修正は12.4です。	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YF	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YI	脆弱性あり。TACに連	

	絡	
12.1YJ	脆弱性あり(最初の修正は12.1EA)	12.1(22)EA13 12.2(44)SE6
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
12.2	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2B	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2BC	脆弱性あり、12.2SCBまたは12.3BCに移行	12.2(33)SCB1 12.3(23)BC6
12.2BW	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2BX	脆弱性あり、12.2SBに移行	12.2(33)SB4
12.2BY	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）

12.2BZ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2CX	脆弱性あり、12.2SCBまたは12.3BCに移行	12.2(33)SCB1 12.3(23)BC6
12.2CY	脆弱性あり、12.2SCBまたは12.3BCに移行	12.2(33)SCB1 12.3(23)BC6
12.2CZ	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2DA	12.2(12)DA14（2009年7月30日に入手可能）	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2DD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2DX	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2EW	脆弱性あり(最初の修正は12.2SG)	12.2(31)SGA9
12.2EWA	脆弱性あり(最初の修正は12.2SG)	12.2(31)SGA9

12.2EX	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2EY	12.2(44)EY	12.2(44)SE6
12.2EZ	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2FX	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2FY	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2FZ	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2IRA	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SRC4（2009年5月18日に入手可能）
12.2IRB	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SRC4（2009年5月18日に入手可能）
12.2IXA	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXB	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXC	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXD	脆弱性あり。12.2IXHの	12.2(18)IXH（2009年

	任意のリリースに移行	3月31日に入手可能）
12.2IXE	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXF	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXG	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2MC	12.2(15)MC2m	12.2(15)MC2m
12.2S	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2SB	12.2(28)SB13 12.2(31)SB14 12.2(33)SB3	12.2(33)SB4
12.2SBC	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4

12.2SCA	脆弱性あり(最初の修正は12.2SCB)	12.2(33)SCB1
12.2SCB	12.2(33)SCB1	12.2(33)SCB1
12.2SE	12.2(50)SE 12.2(46)SE2 12.2(44)SE5	12.2(44)SE6
12.2SEA	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEB	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEC	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SED	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEE	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEF	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEG	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SG	12.2(50)SG	12.2(52)SG（2009年5月15日に入手可能）

12.2SGA	12.2(31)SGA9	12.2(31)SGA9
12.2SL	脆弱性なし	
12.2SM	脆弱性あり。TACに連絡	
12.2SO	脆弱性あり。TACに連絡	
12.2SQ	12.2(44)SQ1	
12.2SRA	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SRD1 12.2(33)SRC4（2009年5月18日に入手可能）
12.2SRB	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SRC4（2009年5月18日に入手可能） 12.2(33)SRD1 12.2(33)SRB5a（2009年4月3日に入手可能）
12.2SRC	12.2(33)SRC4（2009年5月18日に入手可能）	12.2(33)SRC4（2009年5月18日に入手可能）
12.2SRD	脆弱性なし	
12.2STE	脆弱性あり。TACに連絡	
12.2SU	脆弱性あり(最初の修正	12.4(22)T1

	は12.4T)	12.4(15)T9（2009年4月29日に入手可能）
12.2SV	脆弱性あり。TACに連絡	
12.2SVA	脆弱性あり。TACに連絡	
12.2SVC	脆弱性あり。TACに連絡	
12.2SVD	脆弱性あり。TACに連絡	
12.2SVE	脆弱性あり。TACに連絡	
12.2SW	脆弱性あり。TACに連絡	
12.2SX	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXA	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXB	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXD	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16

12.2SXE	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXF	12.2(18)SXF16	12.2(18)SXF16
12.2SXH	12.2(33)SXH5（2009年4月20日に入手可能）	12.2(33)SXH5（2009年4月20日に入手可能）
12.2SXI	脆弱性なし	
12.2SY	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2SZ	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2T	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2TPC	脆弱性あり。TACに連絡	
12.2XA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）

12.2XC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XF	脆弱性あり、12.2SCBまたは12.3BCに移行	12.2(33)SCB1 12.3(23)BC6
12.2XG	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XI	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XJ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）

12.2XK	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XL	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XM	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XN	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SB4 12.2(33)SRD1
12.2XNA	脆弱性あり。12.2SRDの任意のリリースに移行	12.2(33)SRD1
12.2XNB	12.2(33)XNB1	12.2(33)XNB3
12.2XNC	脆弱性なし	
12.2XO	12.2(46)XO	12.2(46)XO
12.2XQ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XR	脆弱性なし	

12.2XS	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XT	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XU	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XV	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XW	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2YA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2YB	脆弱性あり。TACに連絡	
12.2YC	脆弱性あり。TACに連絡	
12.2YD	脆弱性あり。TACに連	

	絡	
12.2YE	脆弱性あり。TACに連絡	
12.2YF	脆弱性あり。TACに連絡	
12.2YG	脆弱性あり。TACに連絡	
12.2YH	脆弱性あり。TACに連絡	
12.2YJ	脆弱性あり。TACに連絡	
12.2YK	脆弱性あり。TACに連絡	
12.2YL	脆弱性あり。TACに連絡	
12.2YM	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2YN	脆弱性あり。TACに連絡	
12.2YO	脆弱性あり。TACに連絡	

12.2YP	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2YQ	脆弱性あり。TACに連絡	
12.2YR	脆弱性あり。TACに連絡	
12.2YS	脆弱性なし	
12.2YT	脆弱性あり。TACに連絡	
12.2YU	脆弱性あり。TACに連絡	
12.2YV	脆弱性あり。TACに連絡	
12.2YW	脆弱性あり。TACに連絡	
12.2YX	脆弱性あり。TACに連絡	
12.2YY	脆弱性あり。TACに連絡	
12.2YZ	脆弱性あり。TACに連絡	

12.2ZA	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2ZB	脆弱性あり。TACに連絡	
12.2ZC	脆弱性あり。TACに連絡	
12.2ZD	脆弱性あり。TACに連絡	
12.2ZE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2ZF	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2ZG	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2ZH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2ZJ	脆弱性あり。TACに連絡	
12.2ZL	脆弱性あり。TACに連	

	絡	
12.2ZP	脆弱性あり。TACに連絡	
12.2ZU	脆弱性あり(最初の修正は12.2SXH)	12.2(33)SXH5（2009年4月20日に入手可能）
12.2ZX	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2ZY	脆弱性あり。TACに連絡	
12.2ZYA	12.2(18)ZYA1	12.2(18)ZYA1
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	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.3B	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3BC	12.3(23)BC6	12.3(23)BC6
12.3BW	脆弱性あり(最初の修正	12.4(22)T1

	は12.4T)	12.4(15)T9（2009年4月29日に入手可能）
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	脆弱性あり。TACに連絡	
12.3JX	脆弱性なし	
12.3T	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3TPC	脆弱性あり。TACに連絡	
12.3VA	脆弱性あり。TACに連絡	
12.3XA	脆弱性あり(最初の修正	12.4(18e)

	は12.4)	12.4(23a)（2009年6月5日に入手可能）
12.3XB	脆弱性あり。TACに連絡	
12.3XC	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XD	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.3XF	脆弱性あり。TACに連絡	
12.3XG	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XI	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.3XJ	脆弱性あり(最初の修正は12.3YX)	12.3(14)YX14
12.3XK	脆弱性あり(最初の修正	12.4(22)T1

	は12.4T)	12.4(15)T9（2009年4月29日に入手可能）
12.3XL	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XQ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XR	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.3XS	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XU	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XW	脆弱性あり(最初の修正は12.3YX)	12.3(14)YX14
12.3XX	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XY	脆弱性あり(最初の修正	12.4(22)T1

	は12.4T)	12.4(15)T9（2009年4月29日に入手可能）
12.3XZ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YA	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YD	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YF	脆弱性あり(最初の修正は12.3YX)	12.3(14)YX14
12.3YG	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YH	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YI	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YJ	脆弱性あり(最初の修正	12.4(22)T1

	は12.4T)	12.4(15)T9（2009年4月29日に入手可能）
12.3YK	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YM	12.3(14)YM13	12.3(14)YM13
12.3YQ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YS	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YT	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YU	脆弱性あり(最初の修正は12.4XB)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YX	12.3(14)YX14	12.3(14)YX14
12.3YZ	脆弱性あり。TACに連絡	
12.3ZA	脆弱性あり(最初の修正	12.4(22)T1

	は12.4T)	12.4(15)T9（2009年4月29日に入手可能）
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(18e) 12.4(23) 12.4(23a)（2009年6月5日に入手可能）	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性あり。TACに連絡	
12.4JMB	脆弱性あり。TACに連絡	
12.4JX	脆弱性なし	
12.4MD	12.4(11)MD7	12.4(11)MD7

12.4MR	12.4(19)MR1	12.4(19)MR2
12.4SW	脆弱性あり。TACに連絡	
12.4T	12.4(20)T2 12.4(15)T8 12.4(22)T 12.4(15)T9（2009年4月29日に入手可能）	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XA	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XB	12.4(15)T8 12.4(20)T2 12.4(15)T9（2009年4月29日に入手可能）	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XC	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XD	12.4(4)XD12（2009年3月27日に入手可能）	12.4(4)XD12（2009年3月27日に入手可能）
12.4XE	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）

12.4XF	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XG	12.4(15)T8 12.4(20)T2	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XJ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XK	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XL	12.4(15)XL4	12.4(15)XL4
12.4XM	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XN	脆弱性あり。TACに連絡	
12.4XP	脆弱性あり。TACに連絡	
12.4XQ	12.4(15)XQ2	12.4(15)XQ2
12.4XR	12.4(15)XR4	12.4(22)T1

		12.4(15)T9（2009年4月29日に入手可能）
12.4XT	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XV	脆弱性あり。TACに連絡	
12.4XW	12.4(11)XW10	12.4(11)XW10
12.4XY	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XZ	12.4(15)XZ2	12.4(15)XZ2
12.4YA	12.4(20)YA2	12.4(20)YA3
12.4YB	脆弱性なし	
12.4YD	脆弱性なし	

推奨事項

$propertyAndFields.get("recommendations")

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からのお問い合わせへの対応の際に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

改訂履歴

リビジョン1.4	2009年6月26日	2009年3月9日の統合修正済みソフトウェアテーブルへの参照を削除。
リビジョン1.3	2009年6月1日	リリース12.4(23a)の公開予定日を更新。
リビジョン1.2	2009年5月1日	リリース12.4(23a)の公開予定日を更新。
リビジョン1.1	2009年4月3日	リリース12.2XR、12.4JL、12.4JK、12.4JX、12.4JDA、12.4JA、12.3JX、12.3JK、12.3JEC、12.3JEB、12.3JEA、12.3JA、12.2JA、および12.2JKは、脆弱性がないことが確認されています。修正済みソフトウェアの表を適宜修正。
リビジョン1.0	2009年3月25日	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。

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。