Cisco IOSソフトウェア複数の機能 巧妙に細工された UDP パケットの脆弱性

High	**アドバイザリーID :** cisco-sa-20090325-udp **初公開日 :** 2009-03-25 16:00 **バージョン 2.0 :** Final **CVSSスコア :** 7.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCsk64158	CVE-2009-0631

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ソフトウェア内の複数の機能は巧妙に細工された UDP パケットの脆弱性から影響を受けます。 影響を受けた機能のうちのどれかが有効に なる場合、不正侵入の成功はインバウンドインターフェイスのブロックされたインプットキューという結果に終ります。 デバイスに宛てた巧妙に細工された UDP パケットだけブロックされるインターフェイスという結果にトランジットトラフィック ブロックしませんインターフェイスを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次のリンクに掲載されます: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp。

注: 2009 年 3月 25 日、Cisco IOS セキュリティ アドバイザリによって組み込まれる書は 8 つのセキュリティ アドバイザリが含まれています。 アドバイザリすべては Cisco IOSソフトウェア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の脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCP サービス拒否の脆弱性
  325-ctcp
- Cisco IOSソフトウェア倍数は IP ソケット脆弱性を特色にします
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- Cisco IOSソフトウェア モバイル IP およびモービル IPv6 脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip
- Cisco IOSソフトウェア Secure Copy（SCP） 特権 拡大脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp
- Cisco IOSソフトウェア Session Initiation Protocol（SIP） サービス拒否の脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip
- Cisco IOSソフトウェア複数の機能によって細工 される TCP シーケンス脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp
- Cisco IOSソフトウェア複数の機能 巧妙に細工された UDP パケットの脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp
- Cisco IOSソフトウェア WebVPN および SSLVPN 脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

脆弱性のある製品

の次の機能実行するとき Cisco IOSソフトウェアの実行するデバイスによって影響を受けるバージョンおよび Cisco IOS XE ソフトウェアは影響を受けています:

- IP サービス レベル契約（IP SLA）（SLA）応答側
- Session Initiation Protocol（SIP; セッション開始プロトコル）
- H.323 Annex E 呼出し シグナリング 転送する
- Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）

方法の詳細はこのアドバイザリの詳細 セクション内で影響を受けた機能がデバイスで有効になるかどうか見る、提供されます。

Cisco製品で動作している Cisco IOS ソフトウェア リリース、管理者をログイン判別し、システムバナーを表示する **" show version " コマンドを**発行することはデバイスにできます。 "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 Ciscoデバイスに**" show version " コマンドが**ありませんし、別の出力を提供しないかもしれません。

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>
```

以下の例は、Cisco 製品にて、IOSリリース 12.4(20)T が稼動し、そのイメージ名が C1841-ADVENTERPRISEK9-M であることを示しています:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (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>
```

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/web/about/security/intelligence/ios-ref.html。

脆弱性を含んでいないことが確認された製品

以下の製品または機能はこの脆弱性の影響を受けません:

- Cisco IOS XR ソフトウェア
- サービス保証エージェント（SAA）
- Response Time Reporter（RTR）
- Cisco 500 シリーズ ワイヤレス アクセス ポイント
- Cisco Aironet 1250 シリーズ
- Cisco Aironet 1240 AG シリーズ
- Cisco Aironet 1230 AG シリーズ
- Cisco Aironet 1200 シリーズ
- Cisco Aironet 1140 シリーズ
- Cisco Aironet 1130 AG シリーズ
- Cisco Aironet 1100 シリーズ
- Cisco Aironet 1500 シリーズ
- Cisco Aironet 1400 シリーズ
- Cisco Aironet 1300 シリーズ
- Cisco AP801（860 および 880 シリーズ ISR で）
- Cisco WMIC（Cisco 3200 Mars で）
- その他の機能かプロトコル on Cisco IOS は影響を受けるために知られていません

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

デバイスは以下に説明される機能のうちのどれかがアクセス可能な関連する UDP ポート番号設定される場合脆弱であり。 脆弱 な コンフィギュレーションのために Cisco IOSデバイスを点検することに加える各機能の場合、管理者はまたいくつかの show コマンドを使用できます UDP サービスを処理する、またはかどうか Cisco IOSデバイスがプロセスを実行した確認するデバイスが影響を受けた UDP ポートで受信すれば。

Cisco IOSソフトウェアの異なるバージョンに Cisco IOSソフトウェア デバイスが受信している UDP ポートを示す異った方法があります。 「show ip sockets」または「show udp」コマンドがこれらのポートを判別するのに使用することができます。 各機能に関しては、1 つの例は影響を受けた UDP ポート番号を示す上記のコマンドを使用して与えられます。

この脆弱性の不正利用の成功はデバイスのインターフェイスをブロックできます。 インターフェイスの種類はこの脆弱性のために無関係です従ってインターフェイスのすべてのイーサネットによって基づくインターフェイス、ATM、シリアル、POS および他の型は影響を受けます。 主要な物理インターフェイスの下のすべての定義された補助的なインターフェイスはメインインターフェイスがブロックされる場合影響を受けています。 攻撃が補助的なインターフェイスに起きる場合、メインインターフェイスはブロックされます。 ブロックされたインターフェイスは非ブロック化されるまで後続パケットを受信することを停止します。 他のインターフェイスはすべて影響を受けていないし、受信および送信パケット続けます。

デバイスのあらゆるインターフェイスの到達可能 構成されたIPアドレスに宛てたパケットだけこの脆弱性を不正利用できます。 トランジットトラフィックはこの脆弱性を不正利用しません。

ブロックされたキューのこの型の現象はきちんと影響を受けたインターフェイス上の接続を確立するルーティング プロトコル (OSPF、EIGRP、BGP、ISIS、等) および MPLS TDP/LDP のようなコントロール プレーン プロトコルの失敗です。 トランジットトラフィックはプロトコル タイマーが影響を受けたデバイスで切れれば影響を受けるかもしれません。

ブロックされたインプットインターフェイスを識別するために、「show interfaces」コマンドを発行し、インプットキュー行を捜して下さい。 インプットキューのサイズは増加し続けることができます。 下記の例の 76 である現在のサイズが等しくまたは大きければより最大サイズ (75) あるデフォルトはインプットキュー ブロックされるかもしれません。

デバイスがコントロール プレーンに向かうトラフィックの高い率を受信するフルキューはただの一時イベントですことは可能性のあるであり。 インターフェイスが実際にブロックされるかどうか確認するために、shutdown interface configuration コマンドでインターフェイスをシャットダウンし、インプットキューを検査して下さい。 インプットキューが 0 パケットを表示する場合、インターフェイスはブロックされます。

```
Router#show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
 Hardware is AmdP2, address is 0050.500e.f1e0 (bia 0050.500e.f1e0)
 Internet address is 192.168.0.1/24
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
 Encapsulation ARPA, loopback not set, keepalive set (10 sec)
```

```
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:41, output 00:00:07, output hang never
 Last clearing of "show interface" counters 00:07:18
 Input queue: 76/75/1091/0 (size/max/drops/flushes); Total output drops: 0
```

IP サービス レベル契約（IP SLA）（SLA）応答側

ユーザ データグラム プロトコル（UDP）のための Cisco IOS IP サービス レベル契約（SLA） 応答側で設定されるデバイスはエコーしますまたはジッタ オペレーション 機能は脆弱です。 応答側として機能するために設定されるどのデバイスでも脆弱です。 以下は 2 脆弱 な コンフィギュレーションを示します。 最初のジェネリック IP SLA 応答側であること:

```
ip sla responder
```

または

```
ip sla monitor responder
```

以下は特定の UDP 応答側が設定されているこの第 2 設定を示します:

```
ip sla responder
ip sla responder udp-echo ipaddress 10.10.10.10 port 1025
```

サービス保証エージェント（SAA）および Response Time Reporter（RTR） 機能は**「ない」**影響を受けたで、**「rtr」**CLI コマンド構文使用します。 脆弱ではない次の例は設定を示したものです、:

```
rtr responder
```

次の例は影響を受けた UDP ポート 1967 が付いているデフォルト IP SLA 制御通信路で受信するデバイスを示したものです。

```
Router#show udp
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 0.0.0.0             0 10.2.6.1        1967   0   0  211   0
```

Cisco IOS IP SLA についてのより詳しい 情報は次のリンクで「Cisco IOS IP SLA コンフィギュレーション ガイドで利用できます、リリース 12.4 - Cisco IOS IP SLA 概要」:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsoverv.html

Session Initiation Protocol（SIP; セッション開始プロトコル）

注: SIP と有効に なる デバイスを持つ顧客向けにまた文書「Cisco Security Advisory 参照して下さい: 次のリンクの Cisco IOS Session Initiation Protocol（SIP） サービス拒否の脆弱性」:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

SIP メッセージを処理する Ciscoデバイスは影響を受けています。 Cisco IOSソフトウェアの最近のバージョンは SIP メッセージをデフォルトで処理しません。 あらゆるオプションでコマンド「

dial-peer voice」による「ダイヤル ピア」を作成することは SIP プロセスを開始し、Cisco IOSソフトウェアを SIP メッセージを処理し始めさせます。 Cisco Call Manager Express 内の複数の機能は、一度設定された ephone のようなまた、自動的に SIP プロセスを開始し、デバイスはために SIP メッセージを処理し始めます。 **「示す IP ソケット」**または**「show udp」**コマンドをで SIP プロセスのプロシージャを確認するためにデバイスが音声コンフィギュレーションを実行しているかどうか推奨します。 以下は影響を受けた設定の 1 つの例です:

```
Router#show udp
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 0.0.0.0            0 10.2.6.1        1967   0   0  211   0
```

注: Cisco IOSソフトウェアのより古いバージョンは Cisco IOSソフトウェアが SIP オペレーションのために設定されないで SIP メッセージを不具合から影響を受けました処理しました。「Cisco Security Advisory を参照して下さい: 次のリンクの SIP のためのサポートの SIP パケット リロード IOSデバイス」:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070131-sip

次の例は SIP メッセージを処理するデフォルトによって影響を受ける UDP ポート 5060 のデバイスを示したものです:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 0.0.0.0            0 192.168.0.2     5060   0   0  211   0
```

SIP についてのより詳しい 情報は、次のリンクで「Cisco IOS SIP コンフィギュレーション ガイド」で利用できます:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/sip_c/sipc1_c/index.htm

H.323 Annex E 呼出し シグナリング 転送する

H.323 をサポートするために設定される Ciscoデバイスは影響を受けています。 影響を受けたプロトコルは UDP 上の H.323 Annex E 呼出し シグナリング 転送するです。 ITU-T 推奨事項 H.323 Annex E は UDP 上の H.225.0 呼び出し信号メッセージを転送するためのシグナリング フレームワークおよびネットワーク プロトコルを記述します。 Cisco IOSソフトウェアの最近のバージョンは H.225.0 UDP ポートをデフォルトでオープンにしません。 あらゆるオプションでコマンド**「dial-peer voice」**による「ダイヤル ピア」を作成することは H.225.0 UDP ポートをオープンにします。 Cisco Call Manager Express 内の複数の機能は、一度設定された ephone のようなまた、自動的に H.323 プロセスを開始し、デバイスはために H.323 パケットを処理し始めます。 **「示す IP ソケット」**または**「show udp」**コマンドをで H.323 プロセスのプロシージャを確認するためにデバイスが音声コンフィギュレーションを実行しているかどうか推奨します。 以下は影響を受けた設定の 1 つの例です:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
```

```
 17 0.0.0.0              0 192.168.0.2      5060   0   0  211   0
```

注: Cisco IOSソフトウェアのより古いバージョンは Cisco IOSソフトウェアが H.323 オペレーションを設定されないで H.323 ポートで聞き取りました不具合から影響を受けました。 Cisco バグ ID を参照して下さい: CSCsb25337 （登録ユーザのみ）

次の例は H.225.0 パケットを処理するデフォルトによって影響を受ける UDP ポート 2517 のデバイスを示したものです:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF

 17 0.0.0.0              0 192.168.0.2      2517   0   0  211   0
```

H.323 についてのより詳しい 情報は、次のリンクで「Cisco IOS H.323 コンフィギュレーション ガイド」で利用できます:
http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_h323_configuration_guide/old_archives_h323/323confg.html

Media Gateway Control Protocol (MGCP; メディア ゲートウェイ コントロール プロトコル)

MGCP 機能で設定されるデバイスは脆弱です。 MGCP はコマンド「mgcp」でグローバルに 有効に なります。 MGCP のためのデフォルト リスニングポートは UDP 2427 です。 次の例は脆弱な 設定を示したものです:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF

 17 0.0.0.0              0 192.168.0.2      2517   0   0  211   0
```

次の例は影響を受けた UDP ポートの MGCP パケットを処理するデバイスを示したものです:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 192.168.0.1     2427 10.66.91.138      2427   0   0  211   0
```

MGCP についてのより詳しい 情報は次のリンクで「Cisco IOS MGCP ゲートウェイ参照」の設定で利用できます:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a008017787b.shtml

この脆弱性は次の Cisco バグ ID で文書化されています: CSCsk64158 （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 CVE-2009-0631 は割り当てられました。

回避策

次の軽減はこの脆弱性のために識別されました; デバイスのあらゆる構成されたIPアドレスに宛て

たパケットだけこの脆弱性を不正利用できます。 トランジットトラフィックはこの脆弱性を不正利用しません。

ディセーブル影響を受けたリスニングポート

影響を受けた機能が必要とならなければ明示的にディセーブルにすることができます。 無効受信 UDP ポートを閉じられました CLI コマンド**「show udp」の**入力によって確認して下さいまたは**「IP ソケット」を示して下さい**。 いくつかの機能は受信 UDP ポートを閉じるために機能をディセーブルにした後デバイスのリロードを必要とするかもしれません。

SIP に関しては TCP サービスだけ必要となる場合受信する UDP をディセーブルにすることは可能性のあるです。 次の例に関連する UDP ポートの受信からの SIP をディセーブルにする方法を示されています。

注: この回避するは統合 Cisco バグ ID CSCsi34903 の Cisco IOSソフトウェアイメージにだけ適用します。

警告： この回避策を MGCP または H.323 呼び出しを処理しているデバイスに適用するとき、デバイスはアクティブ コールが処理されている間処理する停止 SIP を可能にしません。 可能性のある場合の、この対応策はアクティブ コールが簡潔に停止することができるとき Maintenance ウィンドウの間に設定されるはずです。

Enter configuration commands, one per line. Ctrlキーを押しながら Z キーを押して終了します。

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 192.168.0.1     2427 10.66.91.138      2427   0   0  211   0
```

SIP に関しては下記のコマンドで個人的に当たった インターフェイスにプロセスを、結合 することは可能性のあるです。 これにより SIP はこの脆弱性の公開の制限で助けるかもしれない内部インターフェースで受信しますただ:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 192.168.0.1     2427 10.66.91.138      2427   0   0  211   0
```

インフラストラクチャ アクセス コントロール リスト

警告： この脆弱性の機能が転送するとして UDP を利用するので、信頼された IP アドレスからのこれらのポートに ACL をその割り当て通信敗北させるかもしれない送信側の IP アドレスをスプーフィングすることは可能性のあるです。 より有効な緩和策としてユニキャスト RPF を併用することもお勧めします。

ネットワークを通過するトラフィックを遮断することはしばしば困難ですが、インフラストラクチャ デバイスをターゲットとした許可すべきではないトラフィックを特定し、そのようなトラフ

ィックをネットワークの境界で遮断することは可能です。 インフラストラクチャはアクセス コントロール リスト（ACL）（iACLs）ネットワーク セキュリティ 最良 の 方法で、よいネットワーク セキュリティへの長期付加、またこの特定の脆弱性のための回避策として考慮する必要があります。 以下の iACL の例は、Infrastructure access-list の一部として設定されるべきであり、インフラストラクチャ IP アドレスの範囲に含まれる IP アドレスを持つ全ての機器を防御します:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 192.168.0.1     2427 10.66.91.138      2427   0   0  211   0
```

ホワイトペーパー 『Protecting Your Core: インフラストラクチャ 保護はアクセス コントロール リスト（ACL）」インフラストラクチャ 保護 アクセス リストのためのガイドラインおよび推奨される配備手法を示し、次のリンク
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml
で利用できます

コントロール プレーン ポリシング

警告： この脆弱性の機能が転送するとして UDP を利用するので、信頼された IP アドレスからのこれらのポートに ACL をその割り当て通信敗北させるかもしれない送信側の IP アドレスをスプーフィングすることは可能性のあるです。 ユニキャスト RPF はよりよい軽減ソリューションを提供するのに結合で使用されると考慮する必要があります。

コントロール プレーン ポリシング（CoPP）がデバイスに信頼できない UDP トラフィックをブロックするのに使用することができます。 Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T は、CoPP 機能をサポートしています。 管理およびコントロールプレーンを保護するために CoPP を機器に設定し、既存のセキュリティーポリシーとコンフィギュレーションに従って認定されたトラフィックだけがインフラストラクチャデバイス宛に送信されること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その効果を最小限に抑えることができます。 下記の CoPP の例はインフラストラクチャ IP アドレスの範囲内にある IP アドレスを持つ全ての機器を保護するために定義される CoPP の一部として含まれるべき項目です:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 192.168.0.1     2427 10.66.91.138      2427   0   0  211   0
```

上記の CoPP の例では、"permit" アクションであるアクセスコントロールリストエントリ (ACE) に該当し、攻撃である可能性のあるパケットは、policy-map の "drop" 機能により廃棄されますが、一方、"deny" アクション(記載されていません)に該当するパケットは、policy-map の "drop" 機能の影響を受けません。 policy-map の構文は、12.2S と 12.0S Cisco IOS トレインでは異なるので注意が必要です:

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
```

```
 17 192.168.0.1     2427 10.66.91.138      2427   0   0  211   0
```

CoPP 機能の設定および使用のその他の情報は次のリンクで文書で、「コントロール プレーン ポリシング 実装 最良 の 方法」および「Cisco IOS ソフトウェア リリース 12.2 S -コントロール プレーン ポリシング」見つけることができます:
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

ネットワーク内の on Cisco 配置されたデバイスの場合もある追加軽減は次のリンクでこのアドバイザリのための「Cisco 加えました軽減情報」ドキュメントガイドで利用できます:
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090325-sip-and-udp

エクスプロイト 検出

Cisco IOS Embedded Event Manager（EEM） ポリシーのブロックされたインターフェイスキューを検出する 可能性のあるです。 EEM は Cisco IOS デバイスにおけるイベント検知と対応アクション機能を提供します。 EEM は 管理者に対してインターフェースがブロックされたことを email, syslog メッセージ または Simple Network Management Protocol (SNMP) trap により警告することができます。

インターフェースがブロックされたことを管理者に syslog で警告することができるサンプル EEM ポリシーを EEM 専門のオンラインコミュニティ Cisco Beyond で入手することが出来ます。 サンプル スクリプトは次のリンクで入手可能です:
http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=981

EEM についてのより詳しい 情報は次のリンクで Cisco.com から利用できます:
http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.htm

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**
12.0	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0DA	脆弱性あり; first fixed in 12.2DA	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0DB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0DC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0S	12.0(32)S12 12.0(33)S3; 30-APR-2009 で利用可能	12.0(32)S12
12.0SC	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0SL	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0SP	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0ST	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0SX	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0SY	12.0(32)SY8	12.0(32)SY8

12.0SZ	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0T	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0W	脆弱性あり; contact TAC	
12.0WC	脆弱性あり; contact TAC	
12.0WT	脆弱性なし	
12.0XA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XF	脆弱性なし	
12.0XG	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XI	Release prior to 12.0(4)XI2 are vulnerable， releases 12.0(4)XI2 and later are not vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.0XJ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XK	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XL	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XM	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XN	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XQ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XR	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XS	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XT	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XV	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
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; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1AA	脆弱性あり; contact TAC	
12.1AX	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.1AY	脆弱性あり; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
12.1AZ	脆弱性あり; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
12.1CX	脆弱性あり; contact TAC	
12.1DA	脆弱性あり; contact TAC	
12.1DB	脆弱性あり; contact TAC	
12.1DC	脆弱性あり; contact TAC	
12.1E	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.1EA	12.1(22)EA13	12.1(22)EA13
12.1EB	脆弱性あり; contact TAC	
12.1EC	脆弱性あり; first fixed in 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.1EO	脆弱性あり; contact TAC	
12.1EU	脆弱性あり; first fixed in 12.2SG	12.2(31)SGA9
12.1EV	脆弱性あり; contact TAC	
12.1EW	脆弱性あり; 12.2SGA への移行する	12.2(31)SGA9
12.1EX	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1EY	脆弱性あり; contact TAC	
12.1EZ	脆弱性あり; first fixed in 12.2SXF	12.2(18)SX

		F16
12.1GA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1GB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1T	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XF	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XG	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.1XH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XI	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XJ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XL	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XM	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XP	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XQ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XR	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XS	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XT	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.1XU	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XV	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XW	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XX	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XY	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XZ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.1YE	Release prior to 12.1(5)YE6 are vulnerable， releases 12.1(5)YE6 and later are not vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YF	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YI	脆弱性あり; contact TAC	
12.1YJ	脆弱性あり; first fixed in 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; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2B	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2BC	脆弱性あり; 12.2SCB または 12.3BC への移行する	12.2(33)SCB1 12.3(23)BC6
12.2BW	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2BX	脆弱性あり; 12.2SB への移行する	12.2(33)SB4
12.2BY	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-

		2009 で利用可能
12.2BZ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2CX	脆弱性あり; 12.2SCB または 12.3BC への移行する	12.2(33)SCB1 12.3(23)BC6
12.2CY	脆弱性あり; 12.2SCB または 12.3BC への移行する	12.2(33)SCB1 12.3(23)BC6
12.2CZ	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2DA	12.2(12)DA14; 30-JUL-2009 で利用可能	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2DD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2DX	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2EW	脆弱性あり; first fixed in 12.2SG	12.2(31)SGA9
12.2EWA	脆弱性あり; first fixed in 12.2SG	12.2(31)SGA9
12.2EX	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2EY	12.2(44)EY	12.2(44)SE6
12.2EZ	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2FX	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2FY	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2FZ	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2IRA	脆弱性あり; first fixed in 12.2SRC	12.2(33)SR

		C4; 18-MAY-2009 で利用可能
12.2IRB	脆弱性あり; first fixed in 12.2SRC	12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2IXA	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXB	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXC	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXD	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXE	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXF	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXG	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2MB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2MC	12.2(15)MC2m	12.2(15)MC2m
12.2S	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4

12.2SB	12.2(31)SB14 12.2(33)SB3 12.2(28)SB13	12.2(33)SB4
12.2SBC	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2SCA	脆弱性あり; first fixed in 12.2SCB	12.2(33)SCB1
12.2SCB	12.2(33)SCB1	12.2(33)SCB1
12.2SE	12.2(46)SE2 12.2(44)SE5 12.2(50)SE	12.2(44)SE6
12.2SEA	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEB	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEC	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SED	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEE	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEF	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEG	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SG	12.2(50)SG	12.2(52)SG; 15-MAY-2009 で利用可能
12.2SGA	12.2(31)SGA9	12.2(31)SGA9
12.2SL	脆弱性なし	
12.2SM	脆弱性あり; contact TAC	
12.2SO	脆弱性あり; contact TAC	
12.2SQ	12.2(44)SQ1	
12.2SRA	脆弱性あり; first fixed in 12.2SRC	12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2SRB	脆弱性あり; first fixed in 12.2SRC	12.2(33)SRC4; 18-MAY-2009 で利用可能 12.2(33)SRB5a; 3-April-2009 で利用可能

12.2SRC	12.2(33)SRC3	12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2SRD	脆弱性なし	
12.2STE	脆弱性あり; contact TAC	
12.2SU	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2SV	脆弱性あり; contact TAC	
12.2SVA	脆弱性あり; contact TAC	
12.2SVC	脆弱性あり; contact TAC	
12.2SVD	脆弱性あり; contact TAC	
12.2SVE	脆弱性あり; contact TAC	
12.2SW	脆弱性あり; contact TAC	
12.2SX	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXB	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXD	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXE	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXF	12.2(18)SXF16	12.2(18)SXF16
12.2SXH	12.2(33)SXH5; 20-APR-2009 で利用可能	12.2(33)SXH5; 20-APR-2009 で利用可能
12.2SXI	脆弱性なし	
12.2SY	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2SZ	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2T	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2TPC	脆弱性あり; contact TAC	
12.2XA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a);

		05-JUN-2009 で利用可能
12.2XB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XF	脆弱性あり; 12.2SCB または 12.3BC への移行する	12.2(33)SCB1 12.3(23)BC6
12.2XG	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XI	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XJ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XK	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-

		2009 で利用可能
12.2XL	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XM	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XN	脆弱性あり; first fixed in 12.2SRC	12.2(33)SB4 12.2(33)SRD1
12.2XNA	脆弱性あり; migrate to any release in 12.2SRD	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; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XR	脆弱性なし	
12.2XS	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XT	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XU	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XV	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能

12.2XW	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2YA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2YB	脆弱性あり; contact TAC	
12.2YC	脆弱性あり; contact TAC	
12.2YD	脆弱性あり; contact TAC	
12.2YE	脆弱性あり; contact TAC	
12.2YF	脆弱性あり; contact TAC	
12.2YG	脆弱性あり; contact TAC	
12.2YH	脆弱性あり; contact TAC	
12.2YJ	脆弱性あり; contact TAC	
12.2YK	脆弱性あり; contact TAC	
12.2YL	脆弱性あり; contact TAC	
12.2YM	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2YN	脆弱性あり; contact TAC	
12.2YO	脆弱性あり; contact TAC	
12.2YP	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2YQ	脆弱性あり; contact TAC	
12.2YR	脆弱性あり; contact TAC	
12.2YS	脆弱性なし	
12.2YT	脆弱性あり; contact TAC	
12.2YU	脆弱性あり; contact TAC	
12.2YV	脆弱性あり; contact TAC	
12.2YW	脆弱性あり; contact TAC	
12.2YX	脆弱性あり; contact TAC	
12.2YY	脆弱性あり; contact TAC	
12.2YZ	脆弱性あり; contact TAC	
12.2ZA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2ZB	脆弱性あり; contact TAC	
12.2ZC	脆弱性あり; contact TAC	

12.2ZD	脆弱性あり; contact TAC	
12.2ZE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2ZF	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2ZG	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2ZH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2ZJ	脆弱性あり; contact TAC	
12.2ZL	脆弱性あり; contact TAC	
12.2ZP	脆弱性あり; contact TAC	
12.2ZU	脆弱性あり; first fixed in 12.2SXH	12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2ZX	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2ZY	脆弱性あり; contact TAC	
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; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.3B	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3BC	12.3(23)BC6	12.3(23)BC

		6
12.3BW	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
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	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3JL	脆弱性あり; contact TAC	
12.3JX	脆弱性なし	
12.3T	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3TPC	脆弱性あり; contact TAC	
12.3VA	脆弱性あり; contact TAC	
12.3XA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.3XB	脆弱性あり; contact TAC	
12.3XC	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XD	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.3XF	脆弱性あり; contact TAC	
12.3XG	脆弱性あり; first fixed in 12.4T	12.4(22)T1

		12.4(15)T9; 29-APR-2009 で利用可能
12.3XI	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.3XJ	脆弱性あり; first fixed in 12.3YX	12.3(14)YX14
12.3XK	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XL	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XQ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XR	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.3XS	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XU	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XW	脆弱性あり; first fixed in 12.3YX	12.3(14)YX14
12.3XX	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XY	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能

12.3XZ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YA	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YD	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YF	脆弱性あり; first fixed in 12.3YX	12.3(14)YX14
12.3YG	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YH	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YI	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YJ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YK	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YM	12.3(14)YM13	12.3(14)YM13
12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YS	脆弱性あり; first fixed in 12.4T	12.4(22)T1

		12.4(15)T9; 29-APR-2009 で利用可能
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YU	脆弱性あり; first fixed in 12.4XB	12.4(22)T1
12.3YX	12.3(14)YX14	12.3(14)YX14
12.3YZ	脆弱性あり; contact TAC	
12.3ZA	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
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(23) 12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
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; contact TAC	
12.4JMB	脆弱性あり; contact TAC	
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; contact TAC	
12.4T	12.4(15)T8 12.4(20)T2 12.4(22)T 12.4(15)T9; 29-APR-2009 で利用可能	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-

		2009 で利用可能
12.4XB	12.4(15)T8 12.4(20)T2	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XC	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XD	12.4(4)XD12; 27-MAR-2009 で利用可能	12.4(4)XD12; 27-MAR-2009 で利用可能
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XF	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XG	12.4(15)T8 12.4(20)T2 12.4(22)T1	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XK	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XL	12.4(15)XL4	12.4(15)XL4
12.4XM	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XN	脆弱性あり; contact TAC	
12.4XP	脆弱性あり; contact TAC	

12.4XQ	12.4(15)XQ2	12.4(15)XQ2
12.4XR	12.4(15)XR4	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XT	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XV	脆弱性あり; contact TAC	
12.4XW	12.4(11)XW10	12.4(11)XW10
12.4XY	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
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	

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。

この脆弱性は定期的な内部テストの間に Cisco によって検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

改訂履歴

Revision 1.5	2009-June-26	March/09 によって結合される修正済みソフトウェア 表への取除かれた参照。
リビジョン 1.4	2009-June-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。
リビジ	2009-	リリース 12.4(23a) のための更新済期

ョン 1.3	May-1	待された公共有効 日付。
リビジョン 1.2	2009-March-30	具体的には影響を受けない呼出された無線製品
リビジョン 1.1	2009-March-25	影響を受けたリスニングポートを無効にする修正された手順; 回避策を参照して下さい。
リビジョン 1.0	2009-March-25	初回公開リリース

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。