Cisco Security Advisory: Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability

Advisory ID：cisco-sa-20100324-ldp

http://www.cisco.com/JP/support/public/ht/security/107/1076222/cisco-sa-20100324-ldp-j.shtml

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。

Revision 1.1

Last Updated 2010 March 26 1200 UTC (GMT)

For Public Release 2010 March 24 1600 UTC (GMT)

目次

要約
該当製品
詳細
脆弱性スコアの詳細
影響
ソフトウェアのバージョンおよび修正
回避策
修正済みソフトウェアの取得
不正利用事例と公式発表
この通知のステータス：FINAL
情報の配信
更新履歴
シスコのセキュリティ手順

要約

Cisco IOS® ソフトウェア、Cisco IOS XE ソフトウェア、または Cisco IOS XR ソフトウェアを実行しているデバイスが、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）に対応するように設定され、Label Distribution Protocol（LDP）をサポートしている場合、それらのデバイスはサービス拒否（DoS）状態となる可能性があります。

該当バージョンの Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアを実行するデバイスでは、巧妙に細工された LDP UDP パケットによって、リロードが発生する可能性があります

。該当バージョンの Cisco IOS XR ソフトウェアを実行するデバイスでは、巧妙に細工された LDP UDP パケットによって、mpls_ldp プロセスが再起動します。

LDP または Tag Distribution Protocol（TDP）が設定されているシステムは、この脆弱性の影響を受けます。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

この脆弱性による影響を軽減する回避策が利用可能です。

このアドバイザリは次のリンクに掲載されます。
http://www.cisco.com/JP/support/public/ht/security/107/1076222/cisco-sa-20100324-ldp-j.shtml

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。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 日およびそれ以前に公開された全ての 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、次のテーブルをご参照下さい。

http://www.cisco.com/JP/support/public/ht/security/107/1076221/cisco-sa-20100324-bundle-j.shtml

個々の公開リンクは、次のリンクにある「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」内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

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、および Cisco IOS XR ソフトウェアを実行するデバイスで、Targeted LDP hello メッセージまたは Link LDP hello メッセージのいずれかを受信するように設定されている場合、そのデバイスは脆弱です。

MPLS をサポートする全てのバージョンの Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアが、この脆弱性の影響を受けます。Cisco IOS XR ソフトウェア は、3.5.2 より前のリリースが影響を受けます。

脆弱性が存在する製品

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、および Cisco IOS XR ソフトウェアの複数の機能では、デバイスが Targeted LDP hello メッセージまたは Link LDP hello メッセージを受信する必要があります。デバイスが、LDP hello メッセージを受信するように設定されているかどうかを判断する最も確実な方法は、デバイスにログインして、次の操作を実行することです。

1. MPLS フォワーディングが有効かどうかを確認します。
   MPLS フォワーディングが無効なデバイスは、この脆弱性の影響を受けません。

   Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアでは、CLI コマンドの **mpls ip** によって、MPLS フォワーディングがデフォルトで有効です。デバイスで MPLS フォワーディングが無効な場合は、設定内にグローバル設定コマンド **no mpls ip** が含まれています。Cisco IOS ソフトウェアの場合、 デバイスで MPLS フォワーディングが無効かどうかは、**show mpls interface** の出力に表示されます。次では、MPLS フォワーディングが無効な Cisco IOS ソフトウェア デバイスの例を示します。

```
Router#show mpls interface
IP MPLS forwarding is globally disabled on this router.
Individual interface configuration is as follows:

Interface              IP            Tunnel   Operational
Router#
```

Cisco IOS XE ソフトウェアの場合は、**show running-config** の出力にグローバル コマンド **no mpls** が含まれていれば、デバイスは LDP hello メッセージを処理しません。次では、MPLS フォワーディングが無効な Cisco IOS XE ソフトウェア デバイスの例を示します。

```
Router#show running-config | include mpls
no mpls ip
Router#
```

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアでは、MPLS フォワーディングがデフォルトで無効です。

MPLS フォワーディングが有効なデバイスでは、設定内にグローバル設定コマンド **mpls ip** が含まれています。次では、MPLS フォワーディングが有効な Cisco IOS XR ソフトウェアの例を示します。

```
Router#show running-config | include mpls
no mpls ip
Router#
```

次では、MPLS フォワーディングが無効な Cisco IOS XR ソフトウェア デバイスの例を示します。

```
Router#show running-config | include mpls
no mpls ip
Router#
```

MPLS が無効であればデバイスは脆弱性の影響を受けないため、次の手順を実行する必要はありません。

2. デバイスが LDP hello メッセージを受信しているかどうかを確認します。
   デバイスが LDP hello メッセージを受信するように設定されている場合、そのデバイスは脆弱です。

Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェア

デバイスが、LDP hello メッセージを受信するように設定されているかどうかを判断するには、デバイスにログインし、**show ip socket**、**show udp**、または **show control-plane host open-ports** のいずれかのコマンド ライン インターフェイス (CLI) コマンドを実行します。出力に、UDP ポート 646 で listen している IP アドレスが表示される場合、そのデバイスは脆弱です。次では、LDP hello メッセージを受信するように設定されているデバイスの例を示します (show ip socket、show udp、show control-plane host open-ports の各コマンドについて 1 つずつ例を挙げます)。

```
Router#show ip socket
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17   --listen--          192.168.0.1        67   0   0    1   0
 17   --listen--          192.168.0.1        68   0   0    1   0
 17   --listen--          192.168.0.1       711   0   0    1   0
```

```
 17   --listen--          192.168.0.1       646   0   0    1   0
 17   --listen--          192.168.0.1      3503   0   0    1   0
Router#Router#show udp
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17   --listen--          192.168.0.1       123   0   0    1   0
 17   --listen--          192.168.0.1       711   0   0    1   0
 17   --listen--          192.168.0.1       646   0   0    1   0
 17   --listen--          192.168.0.1      3503   0   0    1   0
Router#Router#show control-plane host open-ports
Active internet connections (servers and established)
Prot        Local Address      Foreign Address                 Service    State
 tcp                *:23                *:0                     Telnet   LISTEN
 udp               *:123                *:0                        NTP   LISTEN
 udp               *:646                *:0                  LDP Hello   LISTEN
 udp               *:711                *:0                  TDP Hello   LISTEN
```

Router#Cisco IOS XR ソフトウェア

デバイスが、LDP hello メッセージを受信するように設定されているかどうかを判断するには、デバイスにログインし、CLI コマンド、**show udp brief** を実行します。 出力に、UDP ポート 646 で受信している IP アドレスが表示される場合、そのデバイスは脆弱です。次では、LDP hello メッセージを受信するように設定されているデバイスの例を示します。

```
RP/0/0/CPU0:Router-XR#show udp brief
PCB        Recv-Q Send-Q  Local Address          Foreign Address
0x482609e8      0      0  :::514                 :::0
0x482605f0      0      0  0.0.0.0:514            0.0.0.0:0
0x48260720      0      0  0.0.0.0:646            0.0.0.0:0
```

RP/0/0/CPU0:Router-XR#デバイスが UDP ポート 646 で listen していない場合、そのデバイスは脆弱ではありません。Resource Reservation Protocol (RSVP; リソース リザベーション プロトコル) または Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) のみを使用して、ラベルまたは MPLS スタティック ラベルを配布するように設定されているデバイスは、脆弱ではありません。

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 **show version** コマンドを実行してシステム バナーを表示させます。「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 ソフトウェアが稼動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、続いてバージョンと Cisco IOS ソフトウェア 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** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で IOS ソフトウェア リリース 12.3(26) が稼動し、インストールされているイメージ名が 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   ) 1986-2008 by cisco Systems, Inc.
 Compiled Mon 17-Mar-08 14:39 by dchih

 <output truncated>
```

次の例は、シスコ製品で IOS ソフトウェア 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   ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Cisco IOS ソフトウェアのリリース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/web/about/security/intelligence/ios-ref.html.

脆弱性が存在しない製品

- Cisco NX-OS ソフトウェアは影響を受けません。
- Cisco IOS XR ソフトウェアの 3.5.2 以降のリリー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

MPLS LDP は、MPLS ネットワーク内でピア ラベル スイッチ ルータ（LSR）を有効にすることによって、MPLS ネットワーク内でホップバイホップ フォワーディングをサポートするためのラベル バインディング情報を交換します。

この脆弱性は、Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、および Cisco IOS XR ソフトウェアが、巧妙に細工された LDP パケットを処理する場合に発生します。このアドバイザリの「該当製品」の項で説明しているように、デバイスが LDP hello メッセージを処理するように設定されている場合は、脆弱性の影響を受けます。

巧妙に細工された LDP パケットは、デバイスで受信している任意の IP アドレスの UDP ポート 646 でユニキャストまたはマルチキャスト UDP パケットとして、受信される可能性があります。機器を通過するトラフィックは、この脆弱性のトリガーとはなりません。

注：TDP が設定されたデバイスも、巧妙に細工された LDP パケットを処理するため、脆弱性が存在します。

MPLS および LDP の詳細については、次のリンク先の「Multiprotocol Label Switching (MPLS) Introduction」を参照してください。

http://www.cisco.com/en/US/products/ps6557/products_ios_technology_home.html

この脆弱性は、Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアについては、Cisco Bug ID CSCsz45567（登録ユーザのみ）として、Cisco IOS XR ソフトウェアについては、CSCsj25893（登録ユーザのみ）として文書化されています。この脆弱性に対して Common Vulnerabilities and Exposures（CVE）ID CVE-2010-0576 が割り当てられています。

脆弱性スコアの詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSSは、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコ は次の URL にて CVSS に関する FAQ を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html.

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを次の URL にて提供しています。 http://tools.cisco.com/security/center/cvssCalculator.x.

CSCsz45567: Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability **Calculate the environmental score of**					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsj25893: Cisco IOS XR Software Multiprotocol Label Switching Packet Vulnerability **Calculate the environmental score of**					
CVSS Base Score - **5**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Partial
CVSS Temporal Score - **4.1**					
Exploitability		Remediation Level		Report Confidence	

Functional	Official-Fix	Confirmed

影響

脆弱なバージョンの Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアを実行するデバイスでこの脆弱性が不正利用されると、該当するデバイスでリロードが発生します。

脆弱なバージョンの Cisco IOS XR ソフトウェアを実行するルータで不正利用された場合は、mpls_ldp プロセスが再起動します。

また不正利用を繰り返すことにより、長時間にわたって DoS 状態となる可能性があります。

ソフトウェアのバージョンおよび修正

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/ および本アドバイザリ以降に公開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デバイス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。情報が不明確な場合は、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS のリリース トレインを示します。あるリリース トレインが脆弱である場合、修正を含む最初のリリースは、テーブルの「First Fixed Release」列に示されます（入手可能予想日が示される場合もあります）。「First Fixed Release for all Advisories in 24 March 2010 Bundle Publication」列は、この Cisco IOS セキュリティ アドバイザリの公開時点において公開済みである全ての脆弱性についての修正を含む最初のリリースを示します。可能な限り、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。

Major Release	**Availability of Repaired Releases**	
Affected 12.0-Based Releases	**First Fixed Release for this Advisory**	**First Fixed Release for all Advisories in 24 March 2010 Bundle Publication**
12.0	Not Vulnerable	Not Vulnerable
12.0	Not Vulnerable	Not Vulnerable

DA		
12.0 DB	Not Vulnerable	Not Vulnerable
12.0 DC	Not Vulnerable	Not Vulnerable
12.0S	12.0(32)S15; Available on 25-MAR-10 12.0(33)S6	12.0(32)S15; Available on 25-MAR-10 12.0(33)S6
12.0S C	Not Vulnerable	Not Vulnerable
12.0S L	Vulnerable; first fixed in 12.0S Releases up to and including 12.0(14)SL1 are not vulnerable.	Releases up to and including 12.0(14)SL1 are not vulnerable; First fixed in 12.0S
12.0S P	Not Vulnerable	Not Vulnerable
12.0S T	Releases up to and including 12.0(9)ST are not vulnerable.	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.0S X	Vulnerable; first fixed in 12.0S	Vulnerable; first fixed in 12.0S
12.0S Y	12.0(32)SY11 12.0(32)SY9b	12.0(32)SY11 12.0(32)SY9b
12.0S Z	Vulnerable; first fixed in 12.0S	Vulnerable; first fixed in 12.0S
12.0T	Not Vulnerable	Not Vulnerable
12.0 W	Not Vulnerable	Not Vulnerable
12.0 WC	Not Vulnerable	Not Vulnerable
12.0 WT	Not Vulnerable	Not Vulnerable
12.0X A	Not Vulnerable	Not Vulnerable
12.0X B	Not Vulnerable	Not Vulnerable
12.0X C	Not Vulnerable	Not Vulnerable
12.0X D	Not Vulnerable	Not Vulnerable
12.0X E	Not Vulnerable	Not Vulnerable

12.0XF	Not Vulnerable	Not Vulnerable
12.0XG	Not Vulnerable	Not Vulnerable
12.0XH	Not Vulnerable	Not Vulnerable
12.0XI	Not Vulnerable	Not Vulnerable
12.0XJ	Not Vulnerable	Not Vulnerable
12.0XK	Not Vulnerable	Not Vulnerable
12.0XL	Not Vulnerable	Not Vulnerable
12.0XM	Not Vulnerable	Not Vulnerable
12.0XN	Not Vulnerable	Not Vulnerable
12.0XQ	Not Vulnerable	Not Vulnerable
12.0XR	Not Vulnerable	Not Vulnerable
12.0XS	Not Vulnerable	Not Vulnerable
12.0XT	Not Vulnerable	Not Vulnerable
12.0XV	Not Vulnerable	Not Vulnerable
Affected 12.1-Based Releases	**First Fixed Release for this Advisory**	**First Fixed Release for all Advisories in 24 March 2010 Bundle Publication**
12.1	Not Vulnerable	Not Vulnerable
12.1AA	Not Vulnerable	Not Vulnerable
12.1AX	Vulnerable; first fixed in 12.2SE Releases up to and including 12.1(11)AX are not vulnerable.	Releases up to and including 12.1(11)AX are not vulnerable; first fixed in 12.2SE
12.1AY	Not Vulnerable	Not Vulnerable
12.1AZ	Not Vulnerable	Not Vulnerable
12.1	Not Vulnerable	Not Vulnerable

CX		
12.1 DA	Not Vulnerable	Not Vulnerable
12.1 DB	Not Vulnerable	Not Vulnerable
12.1 DC	Not Vulnerable	Not Vulnerable
12.1E	Vulnerable; first fixed in 12.2SXF Releases up to and including 12.1(7a)E1a are not vulnerable.	Releases up to and including 12.1(7a)E1a are not vulnerable; migrate to any release in 12.2SXF
12.1E A	12.1(22)EA14; Available on 27-JUL-10	Releases up to and including 12.1(6)EA2c are not vulnerable.Releases 12.1(8)EA1c and later are not vulnerable.
12.1E B	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.1E C	Vulnerable; first fixed in 12.2SCB Releases up to and including 12.1(7)EC are not vulnerable.	Releases up to and including 12.1(7)EC are not vulnerable; migrate to 12.2SCB
12.1E O	Releases up to and including 12.1(19)EO6 are not vulnerable.	Releases up to and including 12.1(19)EO6 are not vulnerable.
12.1E U	Not Vulnerable	Not Vulnerable
12.1E V	Not Vulnerable	Not Vulnerable
12.1E W	Not Vulnerable	Not Vulnerable
12.1E X	Vulnerable; migrate to any release in 12.2 Releases up to and including 12.1(6)EX are not vulnerable.	Vulnerable; migrate to any release in 12.2
12.1E Y	Releases up to and including 12.1(7a)EY3 are not vulnerable.	Releases up to and including 12.1(7a)EY3 are not vulnerable.
12.1E	Not Vulnerable	Not Vulnerable

Z		
12.1 GA	Not Vulnerable	Not Vulnerable
12.1 GB	Not Vulnerable	Not Vulnerable
12.1T	Not Vulnerable	Not Vulnerable
12.1X A	Not Vulnerable	Not Vulnerable
12.1X B	Not Vulnerable	Not Vulnerable
12.1X C	Not Vulnerable	Not Vulnerable
12.1X D	Not Vulnerable	Not Vulnerable
12.1X E	Not Vulnerable	Not Vulnerable
12.1X F	Not Vulnerable	Not Vulnerable
12.1X G	Not Vulnerable	Not Vulnerable
12.1X H	Not Vulnerable	Not Vulnerable
12.1X I	Not Vulnerable	Not Vulnerable
12.1X J	Not Vulnerable	Not Vulnerable
12.1X L	Not Vulnerable	Not Vulnerable
12.1X M	Not Vulnerable	Not Vulnerable
12.1X P	Not Vulnerable	Not Vulnerable
12.1X Q	Not Vulnerable	Not Vulnerable
12.1X R	Not Vulnerable	Not Vulnerable
12.1X S	Not Vulnerable	Not Vulnerable
12.1X T	Not Vulnerable	Not Vulnerable
12.1X U	Not Vulnerable	Vulnerable; migrate to any release in 12.2
12.1X V	Note: Releases prior to 12.1(5)XV1 are vulnerable, release 12.1(5)XV1 and later are not vulnerable;	Releases prior to 12.1(5)XV1 are vulnerable, release 12.1(5)XV1 and later are not vulnerable

12.1XW	Not Vulnerable	Not Vulnerable
12.1XX	Not Vulnerable	Not Vulnerable
12.1XY	Not Vulnerable	Not Vulnerable
12.1XZ	Not Vulnerable	Not Vulnerable
12.1YA	Not Vulnerable	Not Vulnerable
12.1YB	Vulnerable; migrate to any release in 12.2	Vulnerable; migrate to any release in 12.2
12.1YC	Not Vulnerable	Not Vulnerable
12.1YD	Vulnerable; migrate to any release in 12.2	Vulnerable; migrate to any release in 12.2
12.1YE	Releases prior to 12.1(5)YE1 are vulnerable, release 12.1(5)YE1 and later are not vulnerable;	Releases prior to 12.1(5)YE6 are vulnerable, release 12.1(5)YE6 and later are not vulnerable.
12.1YF	Not Vulnerable	Not Vulnerable
12.1YH	Not Vulnerable	Not Vulnerable
12.1YI	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.1YJ	Not Vulnerable	Not Vulnerable
Affected 12.2-Based Releases	**First Fixed Release for this Advisory**	**First Fixed Release for all Advisories in 24 March 2010 Bundle Publication**
12.2	Not Vulnerable	Not Vulnerable
12.2B	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BC	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4

		release.
12.2BW	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BX	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BY	Releases prior to 12.2(8)BY are vulnerable, release 12.2(8)BY and later are not vulnerable; first fixed in 12.4	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BZ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2CX	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2CY	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2CZ	Not Vulnerable	Vulnerable; migrate to any release in 12.2SRE
12.2DA	Not Vulnerable	Not Vulnerable
12.2DD	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2DX	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2EW	Not Vulnerable	Not Vulnerable
12.2EWA	Not Vulnerable	Not Vulnerable
12.2EX	Releases up to and including 12.2(37)EX are not vulnerable. Releases 12.2(44)EX and later are not vulnerable; first fixed in 12.2SE	Releases up to and including 12.2(37)EX are not vulnerable. Releases 12.2(44)EX and later are not vulnerable; first fixed in 12.2SE

12.2EY	Releases prior to 12.2(37)EY are vulnerable, release 12.2(37)EY and later are not vulnerable; first fixed in 12.2SE	Releases prior to 12.2(37)EY are vulnerable, release 12.2(37)EY and later are not vulnerable
12.2EZ	Not Vulnerable	Not Vulnerable
12.2FX	Not Vulnerable	Not Vulnerable
12.2FY	Not Vulnerable	Not Vulnerable
12.2FZ	Not Vulnerable	Not Vulnerable
12.2IRA	Vulnerable; first fixed in 12.2SRC	Vulnerable; first fixed in 12.2SRC
12.2IRB	Vulnerable; first fixed in 12.2SRC	Vulnerable; first fixed in 12.2SRC
12.2IRC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IRD	Vulnerable; 12.2(33)IRE, available on 15-April-10	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software	Vulnerable; Contact your support organization per the instructions in

	section of this advisory	Obtaining Fixed Software section of this advisory
12.2IXD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXG	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXH	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2JA	Not Vulnerable	Releases up to and including 12.2(4)JA1 are not vulnerable.
12.2JK	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2MB	Not Vulnerable	Not Vulnerable
12.2MC	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; first fixed in 12.4

12.2 MRA	Not Vulnerable	Not Vulnerable
12.2S	Releases prior to 12.2(30)S are vulnerable, release 12.2(30)S and later are not vulnerable; first fixed in 12.2SB	Releases prior to 12.2(30)S are vulnerable, release 12.2(30)S and later are not vulnerable;
12.2SB	12.2(31)SB18; Available on 24-MAR-10 12.2(33)SB8	12.2(33)SB8 12.2(31)SB18; Available on 24-MAR-10
12.2SBC	Vulnerable; first fixed in 12.2SB	Vulnerable; migrate to any release in 12.2SRE
12.2SCA	Vulnerable; first fixed in 12.2SCB	Vulnerable; first fixed in 12.2SCB
12.2SCB	12.2(33)SCB6	12.2(33)SCB6
12.2SCC	12.2(33)SCC1	12.2(33)SCC1
12.2SCD	Not Vulnerable	Not Vulnerable
12.2SE	12.2(50)SE4; Available on 25-MAR-10	12.2(50)SE4; Available on 25-MAR-10
12.2SEA	Not Vulnerable	Not Vulnerable
12.2SEB	Not Vulnerable	Not Vulnerable
12.2SEC	Not Vulnerable	Not Vulnerable
12.2SED	Vulnerable; first fixed in 12.2SE	Vulnerable; first fixed in 12.2SE
12.2SEE	Vulnerable; first fixed in 12.2SE	Vulnerable; first fixed in 12.2SE
12.2SEF	Not Vulnerable	Not Vulnerable
12.2SEG	Releases prior to 12.2(25)SEG4 are vulnerable, release 12.2(25)SEG4 and later are not vulnerable; first fixed in 12.2SE	Releases prior to 12.2(25)SEG4 are vulnerable, release 12.2(25)SEG4 and later are not vulnerable; first fixed in 12.2SE
12.2SG	Releases up to and including 12.2(31)SG1 are not vulnerable; Release 12.2(40)SG and later are not vulnerable;	Releases up to 12.2(31)SG1 are not vulnerable; releases 12.2(40)SG and later are not vulnerable.

12.2SGA	Not Vulnerable	Not Vulnerable
12.2SL	Not Vulnerable	Not Vulnerable
12.2SM	Not Vulnerable	Not Vulnerable
12.2SO	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2SQ	Not Vulnerable	Not Vulnerable
12.2SRA	Vulnerable; first fixed in 12.2SRD	Vulnerable; first fixed in 12.2SRD
12.2SRB	Vulnerable; first fixed in 12.2SRD	Vulnerable; first fixed in 12.2SRD
12.2SRC	12.2(33)SRC5	12.2(33)SRC5
12.2SRD	12.2(33)SRD3	12.2(33)SRD3
12.2SRE	Not Vulnerable	Not Vulnerable
12.2STE	Not Vulnerable	Not Vulnerable
12.2SU	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2SV	Releases up to and including 12.2(18)SV2 are not vulnerable.	Releases up to and including 12.2(18)SV2 are not vulnerable.
12.2SVA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2SVC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2S	Vulnerable; Contact your	Vulnerable; Contact

VD	support organization per the instructions in Obtaining Fixed Software section of this advisory	your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2SVE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2SW	Releases prior to 12.2(25)SW12 are vulnerable, release 12.2(25)SW12 and later are not vulnerable; migrate to any release in 12.4SW	Releases up to and including 12.2(25)SW3 are not vulnerable. Releases 12.2(25)SW12 and later are not vulnerable; first fixed in 15.0M
12.2SX	Vulnerable; first fixed in 12.2SXF	Vulnerable; first fixed in 12.2SXF
12.2SXA	Vulnerable; first fixed in 12.2SXF	Vulnerable; first fixed in 12.2SXF
12.2SXB	Vulnerable; first fixed in 12.2SXF	Vulnerable; first fixed in 12.2SXF
12.2SXD	Vulnerable; first fixed in 12.2SXF	Vulnerable; first fixed in 12.2SXF
12.2SXE	Vulnerable; first fixed in 12.2SXF	Vulnerable; first fixed in 12.2SXF
12.2SXF	12.2(18)SXF17a	12.2(18)SXF17a
12.2SXH	12.2(33)SXH6	12.2(33)SXH6
12.2SXI	12.2(33)SXI2 12.2(33)SXI2a	12.2(33)SXI2a 12.2(33)SXI3
12.2SY	Vulnerable; first fixed in 12.2SB	Vulnerable; migrate to any release in 12.2SRE
12.2SZ	Vulnerable; first fixed in 12.2SB	Vulnerable; migrate to any release in 12.2SRE
12.2T	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2T	Releases up to and	Vulnerable; Contact

PC	including 12.2(8)TPC10a are not vulnerable.	your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2XA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release. Releases up to and including 12.2(1)XA are not vulnerable.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XB	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XC	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XD	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XE	Not Vulnerable	Not Vulnerable
12.2XF	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XG	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XH	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XI	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XJ	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XK	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.2XL	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XM	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XN	Releases prior to 12.2(33)XN1 are vulnerable, release 12.2(33)XN1 and later are not vulnerable; first fixed in 12.2SRC	Releases prior to 12.2(33)XN1 are vulnerable, release 12.2(33)XN1 and later are not vulnerable; first fixed in 12.2SRC
12.2XNA	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNB	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNC	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XND	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNE	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNF	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XO	Not Vulnerable	Not Vulnerable
12.2XQ	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XR	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XS	Not Vulnerable	Not Vulnerable
12.2XT	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2X	Vulnerable; migrate to any	Vulnerable; migrate to

U	release in 15.0M or a fixed 12.4 release.	any release in 15.0M or a fixed 12.4 release.
12.2XV	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XW	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2YA	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2YB	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YC	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YE	Not Vulnerable	Not Vulnerable
12.2YF	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YG	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of

		this advisory
12.2YH	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YJ	Releases prior to 12.2(8)YJ1 are vulnerable, release 12.2(8)YJ1 and later are not vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YK	Not Vulnerable	Not Vulnerable
12.2YL	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YM	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2YN	Releases prior to 12.2(8)YN1 are vulnerable, release 12.2(8)YN1 and later are not vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YO	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YP	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release. Releases up to and including 12.2(8)YP are not vulnerable.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2YQ	Not Vulnerable	Vulnerable; Contact your support organization per the

		instructions in Obtaining Fixed Software section of this advisory
12.2YR	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YS	Not Vulnerable	Not Vulnerable
12.2YT	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YU	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YV	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YW	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YY	Vulnerable; Contact your support organization per the instructions in	Vulnerable; Contact your support organization per the

	Obtaining Fixed Software section of this advisory	instructions in Obtaining Fixed Software section of this advisory
12.2YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZA	Vulnerable; first fixed in 12.2SXF	Vulnerable; first fixed in 12.2SXF
12.2ZB	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZC	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZE	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2ZF	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2ZG	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2ZH	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.2ZJ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZL	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZP	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZU	Vulnerable; first fixed in 12.2SXH	Vulnerable; first fixed in 12.2SXH
12.2ZX	Vulnerable; first fixed in 12.2SB	Vulnerable; migrate to any release in 12.2SRE
12.2ZY	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZYA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
Affected 12.3-Based Releases	**First Fixed Release for this Advisory**	**First Fixed Release for all Advisories in 24 March 2010 Bundle Publication**
12.3	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.3B	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3BC	Vulnerable; first fixed in 12.2SCB	Vulnerable; first fixed in 12.2SCB
12.3BW	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3EU	Not Vulnerable	Not Vulnerable
12.3JA	Not Vulnerable	Releases prior to 12.3(11)JA5 are vulnerable, release 12.3(11)JA5 and later are not vulnerable
12.3JEA	Not Vulnerable	Releases prior to 12.3(8)JEA4 are vulnerable, release 12.3(8)JEA4 and later are not vulnerable
12.3JEB	Not Vulnerable	Releases prior to 12.3(8)JEB2 are vulnerable, release 12.3(8)JEB2 and later are not vulnerable
12.3JEC	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3JED	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3JK	Releases up to and including 12.3(2)JK3 are not vulnerable. Releases 12.3(8)JK1 and later are not vulnerable; first fixed in 12.4	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3JL	Not Vulnerable	Vulnerable; Contact your support organization per the

		instructions in Obtaining Fixed Software section of this advisory
12.3JX	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3T	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3TPC	Releases up to and including 12.3(4)TPC11a are not vulnerable.	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3VA	Not Vulnerable	Not Vulnerable
12.3XA	Releases up to and including 12.3(2)XA3 are not vulnerable. Releases 12.3(2)XA7 and later are not vulnerable; first fixed in 12.4	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XB	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3XC	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.Releases up to and including 12.3(2)XC4 are not vulnerable.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XD	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XE	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.Releases up to and including	Vulnerable; first fixed in 12.4 Vulnerable; migrate to any release in 15.0M

	12.3(2)XE4 are not vulnerable.	or a fixed 12.4 release.
12.3XF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3XG	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XI	Releases prior to 12.3(7)XI11 are vulnerable, release 12.3(7)XI11 and later are not vulnerable; first fixed in 12.2SB	Releases prior to 12.3(7)XI11 are vulnerable, release 12.3(7)XI11 and later are not vulnerable
12.3XJ	Releases prior to 12.3(7)XJ2 are vulnerable, release 12.3(7)XJ2 and later are not vulnerable; migrate to any release in 12.4XN	Vulnerable; first fixed in 12.4XR
12.3XK	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XL	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XQ	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XR	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.Releases up to and including 12.3(7)XR6 are not vulnerable.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XS	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XU	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4

		release.
12.3XW	Vulnerable; migrate to any release in 12.4XN	Vulnerable; first fixed in 12.4XR
12.3XX	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.Releases up to and including 12.3(8)XX1 are not vulnerable.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XY	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XZ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YA	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YD	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YF	Releases prior to 12.3(11)YF1 are vulnerable, release 12.3(11)YF1 and later are not vulnerable;	Vulnerable; first fixed in 12.4XR
12.3YG	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.Releases up to and including 12.3(8)YG5 are not vulnerable.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YH	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YI	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YJ	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YK	Vulnerable; migrate to any release in 15.0M or a fixed	Vulnerable; migrate to any release in 15.0M

	12.4T release.Releases prior to 12.3(11)YK1 are vulnerable, release 12.3(11)YK1 and later are not vulnerable;	or a fixed 12.4 release.
12.3YM	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YQ	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YS	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.Releases up to and including 12.3(11)YS1 are not vulnerable.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YT	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YU	Vulnerable; migrate to any release in 12.4XB Releases up to and including 12.3(14)YU are not vulnerable.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YX	Releases prior to 12.3(14)YX10 are vulnerable, release 12.3(14)YX10 and later are not vulnerable; migrate to any release in 12.4XN	Vulnerable; first fixed in 12.4XR
12.3YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3ZA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
Affected 12.4-Based	**First Fixed Release for this Advisory**	**First Fixed Release for all Advisories in 24 March 2010 Bundle Publication**

Releases		
12.4	12.4(25c)	12.4(25c) 15.0(1)M1
12.4 GC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4JA	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4JDA	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4JDC	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4JDD	Not Vulnerable	12.4(10b)JDD1
12.4JHA	Not Vulnerable	Not Vulnerable
12.4JK	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4JL	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory

12.4JMA	Not Vulnerable	Releases prior to 12.4(3g)JMA2 are vulnerable, release 12.4(3g)JMA2 and later are not vulnerable
12.4JMB	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4JX	Not Vulnerable	Vulnerable; first fixed in 12.4JA
12.4MD	Not Vulnerable	12.4(24)MD
12.4MDA	Not Vulnerable	12.4(22)MDA2
12.4MR	12.4(20)MR2	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4SW	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4T	12.4(15)T10, 12.4(20)T4, 12.4(22)T3, 12.4(24)T2	12.4(15)T12 12.4(20)T5 12.4(24)T3; Available on 26-MAR-10 12.4(22)T4
12.4XA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XB	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XC	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XD	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4

		release.
12.4XE	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XF	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XG	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XJ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XK	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XL	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4XM	Not Vulnerable	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XN	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4XP	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4XQ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.4XR	12.4(22)XR3	12.4(22)XR3
12.4XT	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XV	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4XW	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XY	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XZ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4YA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4T release.	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4YB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4YD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4YE	12.4(22)YE2	12.4(22)YE2 12.4(24)YE
12.4YG	Not Vulnerable	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed

		Software section of this advisory
Affected 15.0-Based Releases	First Fixed Release for this Advisory	First Fixed Release for all Advisories in 24 March 2010 Bundle Publication
There are no affected 15.0 based releases		
Affected 15.1-Based Releases	First Fixed Release for this Advisory	First Fixed Release for all Advisories in 24 March 2010 Bundle Publication
There are no affected 15.1 based releases		

Cisco IOS XE ソフトウェア

Cisco IOS XE Software Release	First Fixed Release
2.1.x	Vulnerable, Migrate to 2.3.2 or later
2.2.x	Vulnerable, Migrate to 2.3.2 or later
2.3.x	2.3.2
2.4.x	Not Vulnerable
2.5.x	Not Vulnerable
2.6.x	Not Vulnerable

Cisco IOS XR ソフトウェア

この脆弱性は、次の表に従い、適切な Maintenance Upgrade（SMU）を適用することによって対処できます。適切な SMU をインストールした後に、システムをリロードする必要はありません。Cisco IOS XR ソフトウェアおよび SMU の詳細については、次のリンクで「Guidelines for Cisco IOS XR Software」を参照してください。
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8803/ps5845/product_bulletin_c25-478699.htm

Cisco IOS XR Software Version	SMU ID	SMU Name
3.2.X	Vulnerable; Migrate to 3.5.2 or later.	

3.3.X	Vulnerable; Migrate to 3.5.2 or later.	
3.4.0	Vulnerable; Migrate to 3.5.2 or later.	
3.4.1	AA03710 AA03707	c12k-mpls-3.4.1.CSCsj25893 hfr-mpls-3.4.1.CSCsj25893
3.4.2	AA03711 AA03708	c12k-mpls-3.4.2.CSCsj25893 hfr-mpls-3.4.2.CSCsj25893
3.4.3	AA03712 AA03709	c12k-mpls-3.4.3.CSCsj25893 hfr-mpls-3.4.3.CSCsj25893
3.5.2	Not Vulnerable	
3.5.3	Not Vulnerable	
3.5.4	Not Vulnerable	
3.6.X	Not Vulnerable	
3.7.X	Not Vulnerable	
3.8.X	Not Vulnerable	
3.9.X	Not Vulnerable	

回避策

この脆弱性の発現を最小限に抑えるため、対応策を適用することを推奨します。対応策とは、正当なデバイスだけがデバイスに接続できるように設定することです。この緩和策の効果を高めるに、ネットワーク エッジでのアンチスプーフィングを組み合わせる必要があります。この処理が必要になるのは、LDP の hello 転送プロトコルとして UDP も使用されるためです。

デバイスで LDP が不要な場合は、グローバル設定コマンド **no mpls ip** を使用して、MPLS フォワーディングを無効にすることができます。

注：LDP パスワードや MD5 の保護機能では、この脆弱性を防御することはできません。

機器を通過するトラフィックからは、この脆弱性は不正利用されません。この脆弱性を不正利用できるのは、デバイスに着信するパケットのみです。

ネットワーク内のシスコ デバイスに適用可能なその他の緩和策については、次のリンクで、このアドバイザリの付属ドキュメント『Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability』を参照して下さい。 http://www.cisco.com/warp/public/707/cisco-amb-20100324-ldp.shtml.

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： この脆弱性の対象となっている機能は伝送手段として UDP を使用していることから、送

信元 IP アドレスを偽造することも考えられるため、 信用された送信元 IP アドレスからの UDP ポート宛の通信を許可する ACL を設定することによって、 問題を回避できる可能性があります。総合的な対応策として、Unicast Reverse Path Forwarding（Unicast RPF） の使用をお勧めします。

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 ACL（iACL）は、ネットワーク セキュリティのベスト プラクティスであり、特定の脆弱性に対する回避策であると同時に長期に渡って役立つネットワーク セキュリティを付加することができます。次に示す iACL の例は、インフラストラクチャ IP アドレス範囲内にある IP アドレスを持つすべてのデバイスを保護するために配備されたインフラストラクチャ アクセス リストの一部として設定されるべき項目です。

```
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   ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

ホワイトペーパーの『Protecting Your Core：Infrastructure Protection Access Control Lists』は、アクセス リストによってインフラストラクチャ デバイスを保護するガイドラインと、推奨される導入方法が記載されており、次のリンクより入手可能です。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

コントロール プレーン ポリシング

警告： この脆弱性の対象となっている機能は伝送手段として UDP を使用していることから、送信元 IP アドレスを偽造することも考えられるため、 信用された送信元 IP アドレスからの UDP ポート宛の通信のみを許可する ACL を設定することによって、問題を回避できる可能性があります。 総合的な対応策として、Unicast Reverse Path Forwarding（Unicast RPF） の使用をお勧めします。

Control Plane Policing（CoPP; コントロール プレーン ポリシング）は、機器宛の信頼できない UDP トラフィックのブロックに使用できます。CoPP 機能は、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 にてサポートされています。管理およびコントロール プレーンを保護するために CoPP をデバイスに設定し、既存のセキュリティ ポリシーと設定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 ポリシーの例は、インフラストラクチャ IP アドレスの範囲内にある IP アドレスを持つすべてのデバイスを保護するために定義される CoPP の一部として含む必要がある項目です。

```
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   ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

上記の CoPP の例では、「permit」アクションによってアクセス 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 ソフトウェア トレインでは異なるので注意が必要です。

```
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   ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

CoPP の設定と使用法についての追加情報は、次のリンクの『Control Plane Policing Implementation Best Practices』と『Cisco IOS Software Releases 12.2 S - Control Plane Policing』を参照してください。
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

Receive ACL（rACL）

警告： この脆弱性の対象となっている機能は伝送手段として UDP を使用していることから、送信元 IP アドレスを偽造することも考えられるため、 信用された送信元 IP アドレスからの UDP ポート宛の通信のみを許可する ACL を設定することによって、問題を回避できる可能性があります。 総合的な対応策として、Unicast Reverse Path Forwarding（Unicast RPF） の使用をお勧めします。

分散型のプラットフォームにおいて、Cisco12000 シリーズ（GSR）では 12.0(21)S2、Cisco7500 シリーズでは 12.0(24)S、Cisco10720 シリーズでは 12.0(31)Sの IOS ソフトウェアにてサポートされている Receive ACL も選択肢となります。Receive ACL は悪影響を及ぼすトラフィックがルート プロセッサに影響する前に、そのトラフィックからデバイスを防御することができます。Receive ACL は、それが設定されたデバイスだけを防御するようにデザインされています。Cisco 12000、7500、10720 では、通過トラフィックは Receive ACL による影響を受けません。そのため、以下の ACL の例において宛先 IP アドレス「any」が用いられても、自ルータの物理あるいは仮想 IP アドレスのみが参照されます。 Receive ACL は、ネットワーク セキュリティのベスト プラクティスであり、 特定の脆弱性に対する回避策であると同時に 長期に渡って役立つネットワーク セキュリティを付加することができます。ホワイトペーパーの『GSR: Receive Access Control Lists』には、デバイス宛の正当なパケットとそれ以外の遮断されるべきパケットを判断する手法が記載されています。このホワイトペーパーは次のリンクより入手可能です。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml

次の receive path ACL は信頼できるホストからのこのようなタイプのトラフィックを許可するように記述されています

```
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   ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

修正済みソフトウェアの取得

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。ソフトウェアの導入を行う前にお客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項または、Cisco.com Downloads の http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合せいただくことはご遠慮ください。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、シスコのワールドワイド ウェブサイト上のソフトウェア センターからアップグレードを入手することができます。 http://www.cisco.com

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、ネットワークトポロジ、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このお

知らせの URL をご用意ください。サービス契約をご利用でないお客様に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、 http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html を参照してください。

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とその公表は確認しておりません。

この脆弱性はシスコ内部でのテストによって発見されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本アドバイザリの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報の配信

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://www.cisco.com/JP/support/public/ht/security/107/1076222/cisco-sa-20100324-ldp-j.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com

- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。 しかしながら、前述のメーリングリストもしくは ニュースグループに対し 積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報を ご確認いただくことをお勧めいたします。

更新履歴

Revision 1.1	2010-March-26	Update made to iACL example.
Revision 1.0	2010-March-24	Initial public release.

シスコのセキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは http://www.cisco.com/go/psirt/ で確認することができます。