# Cisco Security Advisory: Cisco IOS Software Multicast Source Discovery Protocol Vulnerability

Advisory ID: cisco-sa-20120328-msdp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

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 1.0

For Public Release 2012 March 28 16:00  UTC (GMT)

## 目次



## 要約


Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）実装には、認証されていないリモートの攻撃者が該当デバイスの再起動を引き起こすことのできる脆弱性が存在します。この脆弱性が繰り返し悪用されると、持続的なサービス拒否（DoS）状態になる可能性があります。

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。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

注：2012 年 3 月 28 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 9 件の Cisco Security Advisory が含まれています。各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決する Cisco IOS ソフトウェア リリース、および 2012 年 3 月 にバンドル公開したすべての脆弱性を解決する Cisco IOS ソフトウェア リリースを記載しています。

個々の公開リンクは、次のリンクにある「Cisco Event Response: Semi-Annual 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_mar12.html

# 該当製品

## 脆弱性が存在する製品

次の製品または機能はこの脆弱性の影響を受けます。

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

シスコ製品で稼働している Cisco IOS または Cisco IOS XE 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「Version」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 Cisco IOS ソフトウェア リリース 12.4(20)T が稼働し、インストールされているイメージ名が 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
```

Cisco IOS ソフトウェア リリースの命名規則の追加情報は、以下のリンクのホワイト ペーパー「Cisco IOS and NX-OS Software Reference Guide」 で確認できます。

## 脆弱性が存在しない製品

Cisco IOS XR ソフトウェアは、この脆弱性の影響を受けません。他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

# 詳細

MSDP は、Multiple Protocol Independent Multicast Sparse Mode（PIM-SM）ドメインを接続するためのプロトコルです。MSDP は異なるドメインのランデブー ポイント（RP）すべてに対して、グループのマルチキャスト ソースを知らせます。RP は TCP で MSDP を実行し、マルチキャスト ソースを検出します。

PIM-SM ドメインの RP は、別のドメインの MSDP 対応ルータと MSDP ピアリング関係にあります。ピアリング関係は TCP 接続で確立され、マルチキャスト グループへ送信されるソースのリストが主に交換されます。RP 間の TCP 接続は、基盤となるルーティング システムで確立されます。受信側の RP はソース リストを使ってソース パスを確立します。

このトポロジーの目的は、あるドメインから別のドメインにあるマルチキャスト ソースを検出できるようにすることです。あるマルチキャスト ソースが受信側の存在するドメインと関係がある

場合、マルチキャスト データは PIM-SM の通常のソースツリー作成メカニズムを通じて送信されます。

該当デバイスは、MSDP 設定の外部ピア ルータからカプセル化されたインターネット グループ管理プロトコル ( IGMP ) データを含む MSDP パケットを受信すると、再起動が引き起こされる可能性があります。この脆弱性は、ルータがマルチキャスト グループへ明示的に参加している場合のみ、不正利用できます。MSDP パケットの宛先アドレスはユニキャスト アドレスで、ループバック アドレスを含むすべての IP アドレスに送信することができます。

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。

脆弱性が存在するインターフェイス設定には、明示的に参加するマルチキャスト グループが含まれています。この脆弱性の不正利用が可能となるいくつかの設定例を示します。

!--- SAP リスナー サポート向けに設定されたインターフェイス ( 一般的なマルチキャスト グループ )

```
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
```

!--- マルチキャスト グループへの参加が設定されたインターフェイス

```
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
```

このほか、**show igmp interface** コマンドを使ってインターフェイスがマルチキャスト グループに参加しているかどうかを確認できます。

```
RouterA#show ip igmp interface
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.0.1/24
 IGMP is enabled on interface
 Current IGMP host version is 2
 Current IGMP router version is 2
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Last member query count is 2
 Last member query response interval is 1000 ms
 Inbound IGMP access group is not set
 IGMP activity: 2 joins, 0 leaves
 Multicast routing is disabled on interface
 Multicast TTL threshold is 0
 Multicast groups joined by this system (number of users):
     224.2.127.254(2)  239.255.255.255(1)
```

この脆弱性は、Cisco Bug ID CSCtr28857 ( 登録ユーザ専用 ) に記載されています。この脆弱性に対して Common Vulnerabilities and Exposures ( CVE ) ID CVE-2012-0382 が割り当てられています。

## 脆弱性スコア詳細

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組織の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、自身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。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

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 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

| **CSCtr28857 MSDP-peered Router joined to a multicast group may crash<br>Calculate the environmental score of** | | | | | |
|---|---|---|---|---|---|
| CVSS Base Score - **7.1** | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Network | Medium | None | None | None | Complete |
| CVSS Temporal Score - **5.9** | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

## 影響

この脆弱性が悪用されると、該当するデバイスが再起動する可能性があります。この脆弱性が繰り返し悪用されると、継続的な DoS 状態となる可能性があります。

## ソフトウェア 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場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories and Responses アーカイブと、後続のアドバイザリを参照して、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わせください。

## Cisco IOS ソフトウェア

Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。ある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「First Fixed Release」列に示されます。「First Fixed Release for All Advisories in the March 2012 Bundled Publication」列は、その Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開で公開済みであるすべての脆弱性を修正する最初のリリースを示します。シスコは利用可能な最新のリリースへのアップグレードを推奨します。

Cisco IOS ソフトウェア チェッカーを利用して特定の Cisco IOS ソフトウェア リリースに対応したシスコのセキュリティ アドバイザリを検索することができます。このツールは次の Cisco Security Intelligence Operations（SIO）ポータルで入手できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

| Major Release | Availability of Repaired Releases | |
|---|---|---|
| Affected 12.0-Based Releases | First Fixed Release | First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication |
| 12.0S | 12.0(33)S10 | 12.0(33)S10 |
| 12.0SY | 12.0(32)SY15 | 12.0(32)SY15 |
| 12.0SZ | Vulnerable; First fixed in Release 12.0S | Vulnerable; First fixed in Release 12.0S |
| Affected 12.2-Based Releases | First Fixed Release | First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication |
| 12.2 | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2B | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2BC | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2BW | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2BX | Vulnerable; First fixed in Release 12.2SB | Vulnerable; First fixed in Release 12.2SB |

| | | |
|---|---|---|
| 12.2BY | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2BZ | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2CX | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2CY | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2CZ | Vulnerable; First fixed in Release 12.0S | Vulnerable; First fixed in Release 12.0S |
| 12.2DA | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2DD | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2DX | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2EU | 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. |
| 12.2EW | 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. |
| 12.2EWA | 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. |
| 12.2EX | Vulnerable; First fixed in Release 15.0SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2EY | 12.2(52)EY4<br>12.2(58)EY2 | 12.2(52)EY4 |
| 12.2EZ | Releases prior to 12.2(53)EZ are vulnerable; Releases 12.2(53)EZ and later are not vulnerable.First fixed in Release 15.0SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2F | Not vulnerable | Vulnerable; First fixed in |

| | | |
|---|---|---|
| X | | Release 15.0SE |
| 12.2FY | Not vulnerable | Vulnerable; First fixed in Release 15.0SE |
| 12.2FZ | Vulnerable; First fixed in Release 12.2SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2IRA | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2IRB | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2IRC | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2IRD | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2IRE | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2IRF | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2IRG | 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. |
| 12.2IRH | 12.2(33)IRH1 | 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 section of this advisory. | Vulnerable; contact your support organization per the instructions in 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 | Not vulnerable |
| 12.2JK | Not vulnerable | Not vulnerable |
| 12.2 MB | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2 MC | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2 MRA | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2 MRB | Vulnerable; contact your support organization per the instructions in Obtaining Fixed | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |

| | | |
|---|---|---|
| | Software section of this advisory. | |
| 12.2S | Releases prior to 12.2(30)S are vulnerable; Releases 12.2(30)S and later are not vulnerable.First fixed in Release 12.0S | Releases prior to 12.2(30)S are vulnerable; Releases 12.2(30)S and later are not vulnerable.First fixed in Release 12.0S |
| 12.2SB | 12.2(33)SB12 | 12.2(33)SB12 |
| 12.2SBC | Vulnerable; First fixed in Release 12.2SB | Vulnerable; First fixed in Release 12.2SRE |
| 12.2SCA | Vulnerable; First fixed in Release 12.2SCE | Vulnerable; First fixed in Release 12.2SCE |
| 12.2SCB | Vulnerable; First fixed in Release 12.2SCE | Vulnerable; First fixed in Release 12.2SCE |
| 12.2SCC | Vulnerable; First fixed in Release 12.2SCE | Vulnerable; First fixed in Release 12.2SCE |
| 12.2SCD | Vulnerable; First fixed in Release 12.2SCE | Vulnerable; First fixed in Release 12.2SCE |
| 12.2SCE | 12.2(33)SCE5 | 12.2(33)SCE6 |
| 12.2SCF | 12.2(33)SCF2 | 12.2(33)SCF2 |
| 12.2SE | 12.2(55)SE5 | 12.2(55)SE5 * |
| 12.2SEA | Vulnerable; First fixed in Release 12.2SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2SEB | Vulnerable; First fixed in Release 12.2SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2SEC | Vulnerable; First fixed in Release 12.2SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2SED | Vulnerable; First fixed in Release 12.2SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2SEE | Vulnerable; First fixed in Release 12.2SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2SEF | Not vulnerable | Vulnerable; First fixed in Release 15.0SE |
| 12.2SEG | Releases prior to 12.2(25)SEG4 are vulnerable; Releases 12.2(25)SEG4 and later are not vulnerable.First fixed in Release 15.0SE | Vulnerable; First fixed in Release 15.0SE |
| 12.2SG | 12.2(53)SG7; Available on 07-MAY-12 | 12.2(53)SG7; Available on 07-MAY-12 |
| 12.2S | Vulnerable; contact | Vulnerable; contact your |

| | | |
|---|---|---|
| GA | your support organization per the instructions in Obtaining Fixed Software section of this advisory. | support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.2SL | Not vulnerable | Not vulnerable |
| 12.2SM | 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. |
| 12.2SO | 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 | 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. |
| 12.2SRA | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2SRB | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2SRC | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2SRD | Vulnerable; First fixed in Release 12.2SRE | Vulnerable; First fixed in Release 12.2SRE |
| 12.2SRE | 12.2(33)SRE5 | 12.2(33)SRE6 |
| 12.2STE | Not vulnerable | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.2SU | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 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. |
| 12.2S | Vulnerable; contact | Vulnerable; contact your |

| | | |
|---|---|---|
| VA | your support organization per the instructions in Obtaining Fixed Software section of this advisory. | 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. |
| 12.2SVD | 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. |
| 12.2SVE | 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 | Vulnerable; First fixed in Release 12.4SW | Vulnerable; First fixed in Release 12.4T |
| 12.2SX | 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. |
| 12.2SXA | 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. |
| 12.2SXB | 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 | Vulnerable; contact your |

| | | |
|---|---|---|
| XD | your support organization per the instructions in Obtaining Fixed Software section of this advisory. | support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.2SXE | 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. |
| 12.2SXF | 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. |
| 12.2SXH | 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. |
| 12.2SXI | 12.2(33)SXI9 | 12.2(33)SXI9 |
| 12.2SXJ | 12.2(33)SXJ2 | 12.2(33)SXJ2 |
| 12.2SY | 12.2(50)SY2; Available on 11-JUN-12 | 12.2(50)SY2; Available on 11-JUN-12 |
| 12.2SZ | Vulnerable; First fixed in Release 12.0S | Vulnerable; First fixed in Release 12.0S |
| 12.2T | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2TPC | 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. |
| 12.2XA | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XB | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XC | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |

| | | |
|---|---|---|
| 12.2XD | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XE | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XF | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XG | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XH | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XI | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XJ | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XK | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XL | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XM | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 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 | 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. |
| 12.2XQ | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2X | Releases prior to | Releases prior to |

| | | |
|---|---|---|
| R | 12.2(15)XR are vulnerable; Releases 12.2(15)XR and later are not vulnerable.First fixed in Release 12.4 | 12.2(15)XR are vulnerable; Releases 12.2(15)XR and later are not vulnerable.First fixed in Release 15.0M |
| 12.2XS | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XT | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XU | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XV | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2XW | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2YA | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2YC | 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. |
| 12.2YD | 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 | 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. |
| 12.2YK | 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. |
| 12.2YO | Vulnerable; contact your support organization per the instructions in Obtaining Fixed | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |

| | | |
|---|---|---|
| | Software section of this advisory. | |
| 12.2YP | Vulnerable; First fixed in Release 12.4<br>Releases up to and including 12.2(8)YP are not vulnerable. | Vulnerable; First fixed in Release 15.0M<br>Releases up to and including 12.2(8)YP are 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. |
| 12.2YW | 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. |
| 12.2YX | 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 Obtaining Fixed Software section of this advisory. | Vulnerable; contact your support organization per the 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; 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. |
| 12.2ZB | Vulnerable; contact your support | Vulnerable; contact your support organization per |

| | | |
|---|---|---|
| | organization per the instructions in Obtaining Fixed Software section of this advisory. | the instructions in Obtaining Fixed Software section of this advisory. |
| 12.2ZC | 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. |
| 12.2ZD | 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; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.2ZH | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 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. |
| 12.2ZP | 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. |
| 12.2ZU | 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. |
| 12.2ZX | Vulnerable; First fixed in Release 12.2SB | Vulnerable; First fixed in Release 12.2SRE |
| 12.2ZY | Vulnerable; contact your support organization per the instructions in Obtaining Fixed | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |

| | | |
|---|---|---|
| | 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** | **First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication** |
| 12.3 | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3B | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3BC | Vulnerable; First fixed in Release 12.2SCE | Vulnerable; First fixed in Release 12.2SCE |
| 12.3BW | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3JA | Releases prior to 12.3(4)JA2 are vulnerable; Releases 12.3(4)JA2 and later are not vulnerable.Migrate to any release in 12.4JA | Vulnerable; First fixed in Release 12.4JA |
| 12.3JEA | Not vulnerable | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.3JEB | Not vulnerable | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 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 Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3JL | Not vulnerable | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.3JX | Not vulnerable | Not vulnerable |
| 12.3T | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3TPC | 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. |
| 12.3VA | Not vulnerable | Not vulnerable |
| 12.3XA | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3XB | 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. |
| 12.3XC | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3XD | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3XE | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 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 | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |

| | | |
|---|---|---|
| 12.3XI | Vulnerable; First fixed in Release 12.2SB | Vulnerable; First fixed in Release 12.2SRE |
| 12.3XJ | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3XK | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3XL | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3XQ | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3XR | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3XU | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 12.4T |
| 12.3XW | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3XX | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3XY | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3XZ | Vulnerable; First fixed in Release 12.4 | Vulnerable; First fixed in Release 15.0M |
| 12.3YD | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YF | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YG | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YI | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YJ | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YK | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YM | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YQ | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YS | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YT | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YU | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3YX | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.3Y | Vulnerable; contact | Vulnerable; contact your |

| | | |
|---|---|---|
| Z | your support organization per the instructions in Obtaining Fixed Software section of this advisory. | support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.3ZA | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| **Affected 12.4-Based Releases** | **First Fixed Release** | **First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication** |
| 12.4 | 12.4(25g); Available on 19-SEP-12 | Vulnerable; First fixed in Release 15.0M |
| 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 | 12.4(23c)JA4<br>12.4(25e)JA |
| 12.4JAX | Not vulnerable | Vulnerable; First fixed in Release 12.4JA |
| 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 | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.4JDE | Not vulnerable | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.4JHA | Not vulnerable | Vulnerable; contact your support organization per |

| | | |
|---|---|---|
| | | the instructions in Obtaining Fixed Software section of this advisory. |
| 12.4JHB | Not vulnerable | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 12.4JHC | Not vulnerable | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |
| 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. |
| 12.4JX | Not vulnerable | Vulnerable; First fixed in Release 12.4JA |
| 12.4JY | Not vulnerable | Vulnerable; First fixed in Release 12.4JA |
| 12.4JZ | Not vulnerable | Vulnerable; First fixed in Release 12.4JA |
| 12.4MD | 12.4(24)MD7; Available on 29-Jun-12 | 12.4(22)MD3; Available on 30-MAR-12 |
| 12.4MDA | 12.4(24)MDA11 | 12.4(24)MDA11 |
| 12.4MDB | 12.4(24)MDB5a | 12.4(24)MDB5a |
| 12.4MDC | Not vulnerable | Not vulnerable |
| 12.4MR | 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. |
| 12.4MRA | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this | Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. |

| | | |
|---|---|---|
| | advisory. | |
| 12.4 MRB | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4SW | 12.4(15)SW8a | Vulnerable; First fixed in Release 15.0M |
| 12.4T | 12.4(15)T17<br>12.4(24)T7 | 12.4(15)T17<br>12.4(24)T7 |
| 12.4XA | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XB | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 12.4T |
| 12.4XC | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XD | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XE | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XF | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XG | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XJ | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XK | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XL | 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. |
| 12.4XM | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XN | 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. |
| 12.4XP | 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. |
| 12.4X | Vulnerable; First fixed | Vulnerable; First fixed in |

| | | |
|---|---|---|
| Q | in Release 12.4T | Release 15.0M |
| 12.4XR | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 12.4T |
| 12.4XT | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 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; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XY | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4XZ | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 12.4YA | Vulnerable; First fixed in Release 12.4T | Vulnerable; First fixed in Release 15.0M |
| 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(24)YE3d | 12.4(24)YE3d |
| 12.4YG | 12.4(24)YG4 | 12.4(24)YG4 |
| **Affected 15.0-Based Releases** | **First Fixed Release** | **First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication** |
| 15.0M | 15.0(1)M8 | 15.0(1)M8 |
| 15.0MR | Vulnerable; contact your support | Vulnerable; contact your support organization per |

| | | |
|---|---|---|
| | organization per the instructions in Obtaining Fixed Software section of this advisory. | the instructions in Obtaining Fixed Software section of this advisory. |
| 15.0 MRA | 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. |
| 15.0S | 15.0(1)S5<br>Cisco IOS XE devices: Please see Cisco IOS XE Software Availability | 15.0(1)S5<br>Cisco IOS XE devices: Please see Cisco IOS XE Software Availability |
| 15.0SA | Not vulnerable | Not vulnerable |
| 15.0SE | 15.0(1)SE1<br>15.0(2)SE; Available on 06-AUG-12 | 15.0(1)SE1 |
| 15.0SG | 15.0(2)SG2<br>Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability | 15.0(2)SG2<br>Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability |
| 15.0SY | Not vulnerable | 15.0(1)SY1 |
| 15.0XA | Vulnerable; First fixed in Release 15.1T | Vulnerable; First fixed in Release 15.1T |
| 15.0XO | Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability | Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability |
| **Affected 15.1-Based Releases** | **First Fixed Release** | **First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication** |
| 15.1EY | 15.1(2)EY1a | 15.1(2)EY2 |
| 15.1GC | 15.1(2)GC2 | 15.1(2)GC2 |
| 15.1M | 15.1(4)M2<br>15.1(4)M3a | 15.1(4)M4; Available on 30-MAR-12 |
| 15.1MR | 15.1(1)MR3 | Vulnerable; contact your support organization per |

| | | |
|---|---|---|
| | | the instructions in Obtaining Fixed Software section of this advisory. |
| 15.1S | 15.1(3)S1<br>Cisco IOS XE devices: Please see Cisco IOS XE Software Availability | 15.1(3)S2<br>Cisco IOS XE devices: Please see Cisco IOS XE Software Availability |
| 15.1SG | Not vulnerable<br>Cisco IOS XE devices: Please see Cisco IOS XE Software Availability | Not vulnerable<br>Cisco IOS XE devices: Please see Cisco IOS XE Software Availability |
| 15.1SNG | 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. |
| 15.1SNH | Not vulnerable | Not vulnerable |
| 15.1T | 15.1(1)T5; Available on 18-MAY-12<br>15.1(2)T5; Available on 27-APR-12<br>15.1(3)T3 | 15.1(3)T3 |
| 15.1XB | Vulnerable; First fixed in Release 15.1T | Vulnerable; First fixed in Release 15.1T |
| **Affected 15.2-Based Releases** | **First Fixed Release** | **First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication** |
| 15.2GC | 15.2(1)GC1 | 15.2(1)GC2 |
| 15.2S | Not vulnerable<br>Cisco IOS XE devices: Please see Cisco IOS XE Software Availability | 15.2(1)S1<br>Cisco IOS XE devices: Please see Cisco IOS XE Software Availability |
| 15.2T | 15.2(1)T1<br>15.2(2)T<br>15.2(2)T1 | 15.2(1)T2<br>15.2(2)T1<br>15.2(3)T; Available on 30-MAR-12 |

* Cisco Catalyst 3550 シリーズ スイッチは Internet Key Exchange（IKE; インターネット キー エクスチェンジ）機能をサポートしており、デバイスがレイヤ 3 イメージを実行しているとき

Cisco bug ID CSCts38429 の脆弱性に該当します。ただし、この製品はソフトウェア メンテナンス終了となっています。レイヤ 2 イメージを実行している Cisco 3550 シリーズ SMI スイッチは IKE をサポートしておらず、この脆弱性に該当しません。12.2SE ベースのソフトウェアを稼動しているほかのシスコ デバイスはこの脆弱性に該当しません。

## Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアは、このアドバイザリで説明されている脆弱性の影響を受けます。

| Cisco IOS XE Software Release | First Fixed Release | First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication |
|---|---|---|
| 2.1.x | Vulnerable; migrate to 3.4.1S or later. | Vulnerable; migrate to 3.4.2S or later. |
| 2.2.x | Vulnerable; migrate to 3.4.1S or later. | Vulnerable; migrate to 3.4.2S or later. |
| 2.3.x | Vulnerable; migrate to 3.4.1S or later. | Vulnerable; migrate to 3.4.2S or later. |
| 2.4.x | Vulnerable; migrate to 3.4.1S or later. | Vulnerable; migrate to 3.4.2S or later. |
| 2.5.x | Vulnerable; migrate to 3.4.1S or later. | Vulnerable; migrate to 3.4.2S or later. |
| 2.6.x | Vulnerable; migrate to 3.4.1S or later. | Vulnerable; migrate to 3.4.2S or later. |
| 3.1.xS | Vulnerable; migrate to 3.4.1S or later. | Vulnerable; migrate to 3.4.2S or later. |
| 3.1.xSG | Vulnerable; migrate to 3.2.2SG or later. | Vulnerable; migrate to 3.2.2SG or later. |
| 3.2.xS | Vulnerable; migrate to 3.4.1S or later. | Vulnerable; migrate to 3.4.2S or later. |
| 3.2.xSG | 3.2.2SG | 3.2.2SG |
| 3.3.xS | Vulnerable | Vulnerable; migrate to 3.4.2S or |

| | | |
|---|---|---|
| | ; migrate to 3.4.1S or later. | later. |
| 3.3.xSG | Not Vulnerable | Not Vulnerable |
| 3.4.xS | 3.4.1S | 3.4.2S |
| 3.5.xS | Not vulnerable | 3.5.1S |
| 3.6.xS | Not vulnerable | Not vulnerable |

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、『Cisco IOS XE 2 Release Notes』、『Cisco IOS XE 3S Release Notes』、『Cisco IOS XE 3SG Release Notes』を参照してください。

### Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2012 年 3 月の Cisco IOS Software Security Advisory バンドル公開に含まれている脆弱性の影響を受けません。

## 回避策

MSDP 設定のルータでマルチキャスト グループのメンバシップが不要な場合は、**ip sap listen** または **ip igmp join-group <*マルチキャスト グループのアドレス*>** コマンドをルータ インターフェイスから削除して回避できます。

次に例を示します。

```
RouterA#show ip igmp interface
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.0.1/24
 IGMP is enabled on interface
 Current IGMP host version is 2
 Current IGMP router version is 2
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Last member query count is 2
 Last member query response interval is 1000 ms
 Inbound IGMP access group is not set
 IGMP activity: 2 joins, 0 leaves
 Multicast routing is disabled on interface
 Multicast TTL threshold is 0
 Multicast groups joined by this system (number of users):
     224.2.127.254(2)  239.255.255.255(1)RouterA#show ip igmp interface
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.0.1/24
 IGMP is enabled on interface
 Current IGMP host version is 2
 Current IGMP router version is 2
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
```

```
 Last member query count is 2
 Last member query response interval is 1000 ms
 Inbound IGMP access group is not set
 IGMP activity: 2 joins, 0 leaves
 Multicast routing is disabled on interface
 Multicast TTL threshold is 0
 Multicast groups joined by this system (number of users):
     224.2.127.254(2)  239.255.255.255(1)
```

ルータに MSDP ピアが設定されているかを確認するには、ルータのコマンド プロンプトで **show ip msdp peer** コマンドを実行します。

```
RouterA#show ip igmp interface
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.0.1/24
 IGMP is enabled on interface
 Current IGMP host version is 2
 Current IGMP router version is 2
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Last member query count is 2
 Last member query response interval is 1000 ms
 Inbound IGMP access group is not set
 IGMP activity: 2 joins, 0 leaves
 Multicast routing is disabled on interface
 Multicast TTL threshold is 0
 Multicast groups joined by this system (number of users):
     224.2.127.254(2)  239.255.255.255(1)
```

信頼できない MSDP ピアを設定から削除するには、ルータの設定インターフェイスで **no ip msdp peer <*アドレス*>** または **ip msdp default-peer <*IP* | >** コマンドを実行します。

RouterA(config)# **no ip msdp peer 192.168.0.2**

```
RouterA#show ip igmp interface
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.0.1/24
 IGMP is enabled on interface
 Current IGMP host version is 2
 Current IGMP router version is 2
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Last member query count is 2
 Last member query response interval is 1000 ms
 Inbound IGMP access group is not set
 IGMP activity: 2 joins, 0 leaves
 Multicast routing is disabled on interface
 Multicast TTL threshold is 0
 Multicast groups joined by this system (number of users):
     224.2.127.254(2)  239.255.255.255(1)
```

## 修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。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。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 または http://www.cisco.com/public/sw-center/sw-usingswc.shtml に記載のシスコのソフトウェア ライセンス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 にお問い合わ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、Cisco.com の Software Center 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、適切な処置について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 トポロジー、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。影響製品およびリリース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または修正が最適であるか、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。

- +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、このアドバイザリの 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は TAC を通して無償アップグレードをお求めください。

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、シスコ ワールドワイドお問い合わせ先を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

# 不正利用事例と公式発表

Cisco Product Security Incident Response Team（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、お客様からのお問い合わせへの対応の際に発見されました。

## 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ドキュメント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。

## 情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- 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

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

## 更新履歴

| | | |
|---|---|---|
| Revision 1.0 | 2012-March-28 | Initial public release |

## シスコ 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、Cisco.com 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 Web ページには、シスコのセキュリティ アドバイザリ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。