Cisco IOSソフトウェアのマルチキャストSource Discovery Protocolの脆弱性

High

アドバイザリーID : cisco-sa-20120328-msdp
初公開日 : 2012-03-28 16:00
バージョン 1.0 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID : CSCtr28857

CVE-2012-0382

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアのMulticast Source Discovery Protocol(MSDP)実装における脆弱性により、リモートの認証されていない攻撃者が該当デバイスのリロードを引き起こす可能性があります。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ソフトウェアアップデートをリリースしています。こ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、次のリンクより確認できます。
https://sec.cloudapps.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、このアドバイザリで説明されている脆弱性を修正したCisco IOSソフトウェアリリースと、2012年3月のバンドル公開のすべての脆弱性を修正したCisco IOSソフトウェアリリースが記載されています。

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

該当製品

脆弱性のある製品

次の製品は、この脆弱性に該当します。

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

Cisco IOSソフトウェアリリースまたはCisco IOS XEソフトウェアリリースがシスコ製品で実行されているかどうかを確認するには、管理者がデバイスにログインして show versionコマンドを発行し、システムバナーを表示します。"Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。他のシスコデバイスでは、show version コマンドが存在しなかったり、別の出力が表示されたりします。

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

<#root>

```
Router#
```

show version

```
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

Cisco IOSソフトウェアのリリース命名規則の追加情報は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』で確認できます。

脆弱性を含んでいないことが確認された製品

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

MSDPは、複数のProtocol Independent Multicast(PIM)スパースモード(PIM-SM)ドメインの接続に使用されるプロトコルです。MSDPを使用すると、グループのマルチキャスト送信元を、異なるドメイン内のすべてのランデブーポイント(RP)で認識できます。 RPはTCP上でMSDPを実行し

て、マルチキャスト送信元を検出します。

PIM-SMドメイン内のRPは、別のドメイン内のMSDP対応ルータとMSDPピアリング関係を持ちます。ピアリング関係は、主にマルチキャストグループに送信する送信元のリストが交換されるTCP接続で発生します。RP間のTCP接続は、基盤となるルーティングシステムによって実現されます。受信側RPは、ソースリストを使用してソースパスを確立します。

このトポロジの目的は、ドメインに他のドメインのマルチキャストソースを検出させることです。マルチキャスト送信元がレシーバのあるドメインの対象である場合、マルチキャストデータはPIM-SMの通常のソースツリー構築メカニズム経由で配信されます。

外部MSDPが設定したピアルータから受信した、カプセル化されたInternet Group Management Protocol(IGMP)データを含むMSDPパケットは、該当するデバイスのリロードを引き起こす可能性があります。この脆弱性を不正利用できるのは、ルータがマルチキャストグループに明示的に参加している場合だけです。MSDPパケットの宛先アドレスはユニキャストアドレスであり、ループバックアドレスを含む該当デバイス上の任意のIPアドレスにアドレス指定できます。

通過トラフィックによって、この脆弱性が引き起こされることはありません。

脆弱性のあるインターフェイス設定には、明示的に結合された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を可能にする設定例を次に示します。

!— SAPリスナーサポート用に設定されたインターフェイス（共通のマルチキャストグループ）

```
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
ip pim sparse-mode
ip sap listen
```

! – マルチキャストグループに参加するように設定されたインターフェイス

```
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
ip pim sparse-mode
ip igmp join-group 224.2.127.254
```

また、show igmp interfaceコマンドを使用して、インターフェイスがマルチキャストグループに

加入しているかどうかを確認することもできます。

<#root>

```
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)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としてCVE-2012-0382が割り当てられています。

回避策

MSDPが設定されたルータを使用していて、マルチキャストグループへのメンバーシップを必要としないお客様は、ルータインターフェイスでip sap listenコマンドまたはip igmp join-group <multicast-group address>コマンドを回避策として削除できます。

例：

<#root>

```
RouterA#conf t
  RouterA(config)# interface GigabitEthernet0/0
  RouterA(config-if)# no ip sap listen
  RouterA(config-if)# no ip igmp join-group 224.2.127.254
```

```
  interface GigabitEthernet0/0
  ip address 192.168.0.1 255.255.255.0
  ip pim sparse-mode
```

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

```
RouterA# show ip msdp peer
MSDP Peer 192.168.0.2 (?), AS 100
  Connection status:
    State: Up, Resets: 0, Connection source: none configured
    Uptime(Downtime): 01:23:42, Messages sent/received: 25/24
    Output messages discarded: 0
    Connection and counters cleared 01:15:14 ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 0
    Input queue size: 0, Output queue size: 0
  Message counters:
    RPF Failure count: 0
    SA Messages in/out: 13/8
    SA Requests in: 0
    SA Responses out: 0
    Data Packets in/out: 7/8
```

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

RouterA(config)# no ip msdp peer 192.168.0.2

```
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip pim sparse-mode
```

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、[http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。]

いずれの場合も、アップグレードする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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、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

次のCisco IOSソフトウェアテーブルの各行は、Cisco IOSソフトウェアトレインに対応しています。特定のトレインに脆弱性が存在する場合、修正を含む最も古いリリースが「最初の修正済みリリース」列に表示されます。2012年3月のFirst Fixed Release for All Advisories Bundled Publication列には、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されたすべての脆弱性を修正する最初のリリースが記載されています。シスコでは、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推奨しています。

Cisco IOS Software Checkerを使用すると、特定のCisco IOSソフトウェアリリースに対応するシスコセキュリティアドバイザリを検索できます。このツールは、Cisco Security(SIO)ポータル(https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.x)で利用できます。

メジャーリリース	修正済みリリースの入手可能性	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月の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含まれるすべてのアドバイザリに対する最初の修正リリース
12.0S	12.0(33)S10	12.0(33)S10
12.0SY	12.0(32)SY15	12.0(32)SY15
12.0SZ	脆弱性あり。最初の修正はリリース12.0S	脆弱性あり。最初の修正はリリース12.0S
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月の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含まれるすべてのアドバイザリに対する最初の修正リリース
12.2	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M

12.2B	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2BC	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2BW	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2BX	脆弱性あり。最初の修正はリリース12.2SB	脆弱性あり。最初の修正はリリース12.2SB
12.2BY	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2BZ	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2CX	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2CY	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2CZ	脆弱性あり。最初の修正はリリース12.0S	脆弱性あり。最初の修正はリリース12.0S
12.2DA	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2DD	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2DX	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2EU	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2EW	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせ

	ください。	ください。
12.2EWA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2EX	脆弱性あり。最初の修正はリリース15.0SE	脆弱性あり。最初の修正はリリース15.0SE
12.2EY	12.2(52)EY4 12.2(58)EY2	12.2(52)EY4
12.2EZ	12.2(53)EZより前のリリースには脆弱性があり、12.2(53)EZ以降のリリースには脆弱性はありません。最初の修正はリリース15.0SE	脆弱性あり。最初の修正はリリース15.0SE
12.2FX	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2FY	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2FZ	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2IRA	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRB	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRC	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRD	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRE	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRF	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRG	脆弱性が存在します。	脆弱性が存在します。

	このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IRH	12.2(33)IRH1	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXC	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXD	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせ

	ください。	ください。
12.2IXE	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXF	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXG	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXH	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2JA	脆弱性なし	脆弱性なし
12.2JK	脆弱性なし	脆弱性なし
12.2MB	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2MC	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2MRA	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2MRB	脆弱性が存在します。	脆弱性が存在します。

	このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2S	12.2(30)Sより前のリリースには脆弱性があり、12.2(30)S以降のリリースには脆弱性はありません。最初の修正はリリース12.0S	12.2(30)Sより前のリリースには脆弱性があり、12.2(30)S以降のリリースには脆弱性はありません。最初の修正はリリース12.0S
12.2SB	12.2(33)SB12	12.2(33)SB12
12.2SBC	脆弱性あり。最初の修正はリリース12.2SB	脆弱性あり。最初の修正はリリース12.2SRE
12.2SCA	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE
12.2SCB	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE
12.2SCC	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE
12.2SCD	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース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	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SEB	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SEC	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SED	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SEE	脆弱性あり。最初の修	脆弱性あり。最初の修

	正はリリース12.2SE	正はリリース15.0SE
12.2SEF	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2SEG	12.2(25)SEG4より前のリリースには脆弱性があり、12.2(25)SEG4以降のリリースには脆弱性はありません。最初の修正はリリース15.0SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SG	12.2(53)SG7（2012年5月7日に入手可能）	12.2(53)SG7（2012年5月7日に入手可能）
12.2SGA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SL	脆弱性なし	脆弱性なし
12.2SM	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SO	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SQ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポー	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポー

	ト組織にお問い合わせください。	ト組織にお問い合わせください。
12.2SRA	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRB	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRC	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRE	12.2(33)SRE5	12.2(33)SRE6
12.2STE	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SU	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2SV	12.2(18)SV2 までのリリースには脆弱性はありません。	12.2(18)SV2 までのリリースには脆弱性はありません。
12.2SVA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SVC	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SVD	脆弱性が存在します。	脆弱性が存在します。

	このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SVE	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SW	脆弱性あり。最初の修正はリリース12.4SW	脆弱性あり。最初の修正はリリース12.4T
12.2SX	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SXA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SXB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SXD	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの

	手順に従って、サポート組織にお問い合わせください。	手順に従って、サポート組織にお問い合わせください。
12.2SXE	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SXF	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SXH	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SXI	12.2(33)SXI9	12.2(33)SXI9
12.2日本語	12.2(33)SXJ2	12.2(33)SXJ2
12.2SY	12.2(50)SY2（2012年6月11日に入手可能）	12.2(50)SY2（2012年6月11日に入手可能）
12.2SZ	脆弱性あり。最初の修正はリリース12.0S	脆弱性あり。最初の修正はリリース12.0S
12.2T	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2TPC	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせ

	ください。	ください。
12.2XA	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XB	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XC	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XD	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XE	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XF	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XG	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XH	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XI	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XJ	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XK	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XL	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XM	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XNA	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNB	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNC	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。

12.2XND	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNE	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNF	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XO	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2XQ	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XR	12.2(15)XRより前のリリースには脆弱性があり、12.2(15)XR以降のリリースには脆弱性はありません。最初の修正はリリース12.4	12.2(15)XRより前のリリースには脆弱性があり、12.2(15)XR以降のリリースには脆弱性はありません。最初の修正はリリース15.0M
12.2XS	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XT	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XU	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XV	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2XW	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2YA	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M

12.2YC	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YD	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YE	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YK	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YO	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YP	脆弱性あり。最初の修正はリリース12.4 12.2(8)YPまでのリリースには脆弱性はありません。	脆弱性あり。最初の修正はリリース15.0M 12.2(8)YPまでのリリースには脆弱性はありません。

12.2YT	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YW	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YX	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YY	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2YZ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2ZA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポー	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポー

	ト組織にお問い合わせください。	ト組織にお問い合わせください。
12.2ZB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2ZC	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2ZD	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2ZE	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2ZH	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2ZJ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2ZP	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポー	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポー

	ト組織にお問い合わせください。	ト組織にお問い合わせください。
12.2ZU	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2ZX	脆弱性あり。最初の修正はリリース12.2SB	脆弱性あり。最初の修正はリリース12.2SRE
12.2ZY	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2ZYA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
Affected 12.3-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月の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含まれるすべてのアドバイザリに対する最初の修正リリース
12.3	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3B	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3BC	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE
12.3BW	脆弱性あり。最初の修	脆弱性あり。最初の修

	正はリリース12.4	正はリリース15.0M
12.3JA	12.3(4)JA2より前のリリースには脆弱性があり、12.3(4)JA2以降のリリースには脆弱性はありません。 12.4JAの任意のリリースに移行	脆弱性あり。最初の修正はリリース12.4JA
12.3JEA	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3JEB	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3JEC	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3JED	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3JK	12.3(2)JK3 までのリリースには脆弱性はありません。 12.3(8)JK1以降のリリ	脆弱性あり。最初の修正はリリース15.0M

	ースには脆弱性はありません。最初の修正はリリース12.4	
12.3JL	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3JX	脆弱性なし	脆弱性なし
12.3T	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3TPC	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3VA	脆弱性なし	脆弱性なし
12.3XA	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3XC	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XD	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XE	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XF	脆弱性が存在します。このアドバイザリの「	脆弱性が存在します。このアドバイザリの「

	修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3XG	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XI	脆弱性あり。最初の修正はリリース12.2SB	脆弱性あり。最初の修正はリリース12.2SRE
12.3XJ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3XK	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XL	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3XQ	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XR	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XU	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.3XW	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3XX	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XY	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XZ	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3YD	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YF	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YG	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YI	脆弱性あり。最初の修	脆弱性あり。最初の修

	正はリリース12.4T	正はリリース15.0M
12.3YJ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YK	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YM	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YQ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YS	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YT	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YU	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YX	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YZ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3ZA	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月の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含まれるすべてのアドバイザリに対する最初の修正リリース
12.4	12.4(25g)（2012年9月19日に入手可能）	脆弱性あり。最初の修正はリリース15.0M
12.4GC	脆弱性が存在します。このアドバイザリの「	脆弱性が存在します。このアドバイザリの「

	修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JA	脆弱性なし	12.4(23c)JA4 12.4(25e)JA
12.4JAX	脆弱性なし	脆弱性あり。最初の修正はリリース12.4JA
12.4JDA	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JDC	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JDD	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JDE	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JHA	脆弱性なし	脆弱性が存在します。このアドバイザリの「

		修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JHB	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JHC	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JK	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JL	脆弱性なし	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JX	脆弱性なし	脆弱性あり。最初の修正はリリース12.4JA
12.4JY	脆弱性なし	脆弱性あり。最初の修正はリリース12.4JA
12.4JZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4JA

12.4MD	12.4(24)MD7（2012年6月29日に入手可能）	12.4(22)MD3（2012年3月30日に入手可能）
12.4MDA	12.4(24)MDA11	12.4(24)MDA11
12.4MDB	12.4(24)MDB5a	12.4(24)MDB5a
12.4MDC	脆弱性なし	脆弱性なし
12.4MR	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
1240万	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4MRB	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4SW	12.4(15)SW8a	脆弱性あり。最初の修正はリリース15.0M
12.4T	12.4(15)T17 12.4(24)T7	12.4(15)T17 12.4(24)T7
12.4XA	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XB	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4XC	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XD	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XE	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XF	脆弱性あり。最初の修	脆弱性あり。最初の修

	正はリリース12.4T	正はリリース15.0M
12.4XG	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XJ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XK	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XL	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4XM	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XN	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4XP	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4XQ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XR	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4XT	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XV	脆弱性が存在します。このアドバイザリの「	脆弱性が存在します。このアドバイザリの「

	修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4XW	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XY	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XZ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4YA	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4YB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4YD	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4YE	12.4(24)YE3d	12.4(24)YE3d
12.4YG	12.4(24)YG4	12.4(24)YG4
影響を受ける 15.0 ベースのリリース	First Fixed Release（修正された最初のリリース）	2012年3月の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含まれるすべてのアドバイザリに対する最初の修正リリース
15.0M	15.0(1)M8	15.0(1)M8
15.0MR	脆弱性が存在します。	脆弱性が存在します。

	このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.0MRA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.0秒	15.0(1)S5 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.0(1)S5 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.0SA	脆弱性なし	脆弱性なし
15.0SE	15.0(1)SE1 15.0(2)SE（2012年8月6日に入手可能）	15.0(1)SE1
15.0SG	15.0(2)SG2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.0(2)SG2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.0SY	脆弱性なし	15.0(1)SY1
15.0XA	脆弱性あり。最初の修正はリリース15.1T	脆弱性あり。最初の修正はリリース15.1T
15.0XO	Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
影響を受ける 15.1	First Fixed Release（修正された	2012年3月のCisco IOSソフトウェアセキ

ベースのリリース	最初のリリース）	ユリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
15.1EY	15.1(2)EY1a	15.1(2)EY2
15.1GC	15.1(2)GC2	15.1(2)GC2
1,510万	15.1(4)M2 15.1(4)M3a	15.1(4)M4（2012年3月30日に入手可能）
15.1MR	15.1(1)MR3	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1S	15.1(3)S1 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.1(3)S2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.1SG	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.1SNG	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1SNH	脆弱性なし	脆弱性なし
15.1T	15.1(1)T5（2012年5月18日に入手可能） 15.1(2)T5（2012年	15.1(3)T3

	4月27日に入手可能） 15.1(3)T3	
15.1XB	脆弱性あり。最初の修正はリリース15.1T	脆弱性あり。最初の修正はリリース15.1T
Affected 15.2-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月の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含まれるすべてのアドバイザリに対する最初の修正リリース
15.2GC	15.2(1)GC1	15.2(1)GC2
15.2秒	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.2(1)S1 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.2T	15.2(1)T1 15.2(2)T 15.2(2)T1	15.2(1)T2 15.2(2)T1 15.2(3)T（2012年3月30日に入手可能）

* Cisco Catalyst 3550シリーズスイッチは、インターネットキーエクスチェンジ(IKE)機能をサポートしており、デバイスでレイヤ3イメージを実行している場合はCisco Bug ID CSCts38429に対して脆弱です。ただし、この製品はソフトウェアメンテナンスが終了しています。 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をサポートしていないため、脆弱ではありません。 12.2SEベースのソフトウェアを実行する他のシスコデバイスには、この脆弱性は存在しません。

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 ソフトウェア リリース	First Fixed Release（修正された最初のリリース）	2012年3月の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含まれるすべてのアドバイザリに対する最初の修正リリース
2.1.x	脆弱性あり。	脆弱性あり。3.4.2S以降

	3.4.1S以降に移行してください。	に移行してください。
2.2.x	脆弱性あり。3.4.1S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
2.3.x	脆弱性あり。3.4.1S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
2.4.x	脆弱性あり。3.4.1S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
2.5.x	脆弱性あり。3.4.1S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
2.6.x	脆弱性あり。3.4.1S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
3.1.xS	脆弱性あり。3.4.1S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
3.1.xSG	脆弱性あり。3.2.2SG以降に移行してください。	脆弱性あり。3.2.2SG以降に移行してください。
3.2.xS	脆弱性あり。3.4.1S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
3.2.xSG	3.2.2SG	3.2.2SG
3.3.xS	脆弱性あり。3.4.1S以降に移	脆弱性あり。3.4.2S以降に移行してください。

	行してください。	
3.3.xSG	脆弱性なし	脆弱性なし
3.4.xS	3.4.1S	3.4.2S
3.5.xS	脆弱性なし	3.5.1S
3.6.xS	脆弱性なし	脆弱性なし

Cisco IOS ソフトウェア リリースへの Cisco IOS XE 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」、および「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。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

この脆弱性は、お客様のサービスリクエストのトラブルシューティング中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

改訂履歴

リビジョン 1.0	2012年3月28日	初版リリース

利用規約

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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