Cisco IOSソフトウェアのデータリンクスイッチングの脆弱性

アドバイザリーID : cisco-sa-20110928-dlsw CVE-2011-0945
初公開日 : 2011-09-28 16:00
最終更新日 : 2012-09-21 19:18
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCth69364

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ソフトウェアには、Data-Link Switching（DLSw；データリンクスイッチング）機能のメモリリークの脆弱性があり、巧妙に細工されたIP Protocol 91パケットの処理時にデバイスのリロードが発生す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。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw で公開されています。

注： 2011年9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10件のCisco Security Advisoryが含まれています。9件のアドバイザリはCisco IOSソフトウェアの脆弱性に対処するもので、1件はCisco Unified Communications Managerの脆弱性に対処するものです。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、2011年9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: Semiannual 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_sep11.html

該当製品

脆弱性のある製品

DLSwのpromiscuous機能が有効になっているCisco IOSデバイスは、このアドバイザリに記載されている脆弱性の影響を受けます。DLSwのpromiscuous機能が有効になっているデバイスには、promiscuousキーワードを使用してローカルDLSwピアを定義している設定に1行が含まれています。この設定を確認するには、show running-configコマンドを発行します。DLSwの無差別モード機能が有効に設定されたシステムには、次のような行が含まれています。

```
dlsw local-peer promiscuous
```

または

```
dlsw local-peer peer-id <IP address> promiscuous
```

Cisco IOSデバイスで実行されているソフトウェアを確認するには、デバイスにログインし、show versionコマンドを発行してシステムバナーを表示します。Cisco IOSソフトウェアは、「Cisco Internetwork Operating System Software」または「Cisco IOS Software」と表示されます。 他のシスコデバイスにはshow versionコマンドがないか、異なる出力が返されます。

次の例は、IOSバージョン15.0(1)M1を実行しているデバイスからの出力を示しています。

<#root>

```
Router>
```

show version

```
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 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、ホワイトペーパー『Cisco IOS and NX-OS Software Reference Guide』(http://www.cisco.com/web/about/security/intelligence/ios-ref.html)を参照してください。

脆弱性を含んでいないことが確認された製品

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

DLSwは、IPネットワーク上でIBM Systems Network Architecture(SNA)およびネットワークBIOS(NetBIOS)トラフィックを転送する手段を提供します。シスコのDLSw over Fast Sequence Transport(FST)の実装では、IPプロトコル91を使用します。無差別DLSw機能を使用すると、ローカルピアは、静的に設定されていないリモートピアとの接続を確立できます。

DLSw用に設定されたCisco IOSデバイスは、IPプロトコル91パケットをリッスンします。DLSwの設定に応じて、UDPポート2067、および1つ以上のTCPポートも開くことができます。このドキュメントで説明されている脆弱性は、IPプロトコル91を介してのみ不正利用でき、UDPまたはTCPトランスポートを使用して不正利用することはできません。

静的に設定されたDLSwピアのみを持つデバイスは、この脆弱性の影響を受けません。

この脆弱性は、Cisco Bug ID CSCth69364(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2011-0945が割り当てられています。

回避策

この脆弱性は、コントロールプレーンポリシング(CoPP)を使用して、有効なピアから送信されたIPプロトコル91のパケットのみを許可することで軽減できます。

ネットワーク内のCiscoデバイスに導入できる緩和テクニックについては、このアドバイザリに関連するCisco適用対応策速報(https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110928-dlsw)を参照してください。

コントロール プレーン ポリシング

コントロールプレーンポリシング(CoPP)を使用して、該当デバイスに送信される信頼できないIPプロトコル91パケットをブロックすることができます。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でサポートされています。CoPPは、管理プレーンとコントロールプレーンを保護するようにデバイス上に設定できます。これにより、既存のセキュリティポリシーと設定に従って、インフラストラクチャデバイスに送信される認可されたトラフィックのみを明示的に許可し、レート制限することで、インフラストラクチャへの直接攻撃のリスクと効果を最小限に抑えることができます。次の例では、192.168.100.1を使用して信頼できるホストを表しており、ネットワークに適用できます。

```
!-- Deny FST traffic on IP protocol 91 from trusted
!-- hosts to all IP addresses configured on all interfaces of the affected device
!-- so that it will be allowed by the CoPP feature
```

```
access-list 111 deny 91 host 192.168.100.1 any


!-- Permit all other FST traffic on IP protocol 91
!-- sent to all IP addresses configured on all interfaces of the affected
!-- device so that it will be policed and dropped by the CoPP feature


access-list 111 permit 91 any any


!-- Permit (Police or Drop)/Deny (Allow) all other Layer3
!-- and Layer4 traffic in accordance with existing security
!-- policies and configurations for traffic that is authorized
!-- to be sent to infrastructure devices

!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature


class-map match-all drop-fst-91-class
  match access-group 111


!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.


policy-map input-CoPP-policy
  class drop-fst-91-class
    drop


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


control-plane
  service-policy input input-CoPP-policy
```

上記のCoPPの例では、access control list entries（ACE；アクセスコントロールリストエントリ）で「permit」アクションが指定されている潜在的な悪用パケットと一致するものが、ポリシーマップの「drop」機能によって廃棄されます。一方、denyアクション（非表示）と一致するパケットは、ポリシーマップのdrop機能の影響を受けません。Cisco IOSトレイン12.2Sおよび12.0Sでは、ポリシーマップの構文が異なることに注意してください。次に例を示します。

```
policy-map input-CoPP-policy
  class drop-fst-91-class
    police 32000 1500 1500 conform-action drop exceed-action drop
```

CoPP機能の詳細については、『Control Plane Policing Implementation Best Practices』を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

また、Cisco IOS Software Checkerは、Cisco Security(SIO)ポータル(https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.x)でも入手できます。特定のバージョンのCisco IOSソフトウェアに影響を与えるセキュリティアドバイザリを確認するための機能がいくつかあります。

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「このアドバイザリの最初の修正済みリリース」列に記載されます。2011年9月の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には、Cisco IOSソフトウェアセキュリティアドバイザリのバンドル公開に含まれるすべての公開済みの脆弱性を修正する最初の修正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。

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）	2011年9月の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
該当する12.0ベースのリリースはありません		
Affected 12.1-	First Fixed Release（修正	2011年9月のバンドル公開に含まれるすべてのアドバ

Based Releases	された最初のリリース）	イザリに対する最初の修正リリース
12.1E	脆弱性あり。最初の修正はリリース12.2SXF	脆弱性あり。最初の修正はリリース12.2SXF
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）	2011年9月の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12.4
12.2B	脆弱性あり。最初の修正はリリース12.4 12.2(2)B7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12.4
12.2BC	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2BW	脆弱性なし	脆弱性なし
12.2BX	脆弱性あり。最初の修正はリリース12.2SB 12.2(15)BXまでのリリースには	脆弱性あり。最初の修正はリリース12.2SB

	脆弱性はありません。	
12.2BY	脆弱性なし	脆弱性なし
12.2BZ	脆弱性なし	脆弱性なし
12.2CX	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2CY	脆弱性なし	脆弱性なし
12.2CZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SB
12.2DA	脆弱性なし	脆弱性なし
12.2DD	脆弱性なし	脆弱性なし
12.2DX	脆弱性なし	脆弱性なし
12.2EU	脆弱性なし	脆弱性なし
12.2EW	脆弱性なし	12.2(20)EW4までのリリースには脆弱性はありません。
12.2EWA	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。

12.2EX	脆弱性なし	12.2(55)EX3
12.2EY	脆弱性なし	12.2(58)EY
12.2EZ	脆弱性なし	脆弱性あり。15.0SEの任意のリリースに移行
12.2FX	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2FY	脆弱性なし	脆弱性あり(最初の修正はリリース12.2EX)
12.2FZ	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2IRA	脆弱性あり。12.2IRGの任意のリリースに移行	脆弱性あり。12.2IRGの任意のリリースに移行
12.2IRB	脆弱性あり。12.2IRGの任意のリリースに移行	脆弱性あり。12.2IRGの任意のリリースに移行
12.2IRC	脆弱性あり。12.2IRGの任意のリリースに移行	脆弱性あり。12.2IRGの任意のリリースに移行
12.2IRD	12.2(33)IRD1	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。
12.2IRE	12.2(33)IRE3	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。
12.2IRF	脆弱性あり。12.2IRGの任意のリリースに移行	脆弱性あり。12.2IRGの任意のリリースに移行
12.2IRG	脆弱性なし	脆弱性なし
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	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。

	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。
12.2IXE	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	脆弱性が存在します。このアドバイザリの「修正済み

	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。	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	脆弱性なし	脆弱性なし

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12.4
12.2MRA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRD
12.2MRB	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。
12.2S	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12.2SB	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12.2SB
12.2SB	12.2(31)SB20 12.2(33)SB10	12.2(31)SB20 12.2(33)SB10
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12.2SB
12.2SCA	脆弱性あり。最初の修正はリリース12.2SCC	脆弱性あり。最初の修正はリリース12.2SCC

12.2SCB	脆弱性あり。最初の修正はリリース12.2SCC	脆弱性あり。最初の修正はリリース12.2SCC
12.2SCC	12.2(33)SCC7	12.2(33)SCC7
12.2SCD	12.2(33)SCD6 12.2(33)SCD7	12.2(33)SCD6
12.2SCE	12.2(33)SCE1 12.2(33)SCE2	12.2(33)SCE112.2(33)SCE2
12.2SCF	脆弱性なし	脆弱性なし
12.2SE	脆弱性なし	12.2(55)SE312.2(58)SE
12.2SEA	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SEB	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SEC	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SED	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SEE	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)

12.2SEF	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SEG	脆弱性なし	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12.2EX
12.2SG	12.2(40)SGより前のリリースには脆弱性があり、12.2(40)SG以降のリリースには脆弱性はありません。	12.2(53)SG4より前のリリースには脆弱性があり、12.2(53)SG4以降のリリースには脆弱性はありません。
12.2SGA	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。
12.2SL	脆弱性なし	脆弱性なし
12.2SM	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。
12.2SO	脆弱性なし	脆弱性なし

12.2SQ	脆弱性なし	12.2(50)SQ3
12.2SRA	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRD
12.2SRB	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRD
12.2SRC	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRD
12.2SRD	12.2(33)SRD6	12.2(33)SRD6
12.2SRE	12.2(33)SRE3	12.2(33)SRE4
12.2STE	脆弱性なし	脆弱性なし
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12.4
12.2SV	12.2(29a)SVより前のリリースには脆弱性があり、12.2(29a)SV以降のリリースには脆弱性はありません。12.2SVDの任意のリリースに移行	12.2(29a)SVより前のリリースには脆弱性があり、12.2(29a)SV以降のリリースには脆弱性はありません。12.2SVDの任意のリリースに移行

12.2SVA	脆弱性なし	脆弱性なし
12.2SVC	脆弱性なし	脆弱性なし
12.2SVD	脆弱性なし	脆弱性なし
12.2SVE	脆弱性なし	脆弱性なし
12.2SW	12.2(25)SW12より前のリリースには脆弱性があり、12.2(25)SW12以降のリリースには脆弱性はありません。	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。
12.2SX	脆弱性あり。最初の修正はリリース12.2SXF	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXA	脆弱性あり。最初の修正はリリース12.2SXF	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXB	脆弱性あり。最初の修正はリリース12.2SXF	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXD	脆弱性あり。最初の修正はリリース12.2SXF	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXE	脆弱性あり。最	脆弱性あり。最初の修正は

	初の修正はリリース12.2SXF	リリース12.2SXF
12.2SXF	12.2(18)SXF17b	12.2(18)SXF17b
12.2SXH	12.2(33)SXH8a	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)SXI6	12.2(33)SXI6
12.2日本語	脆弱性なし	12.2(33)SXJ1
12.2SY	12.2(50)SY	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。
12.2SZ	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
12.2T	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12.4
12.2TPC	脆弱性が存在します。このアドバイザリの「修	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

	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。	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。
12.2XA	脆弱性なし	脆弱性なし
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12.4
12.2XC	脆弱性なし	脆弱性なし
12.2XD	脆弱性なし	脆弱性なし
12.2XE	脆弱性なし	脆弱性なし
12.2XF	脆弱性なし	脆弱性なし
12.2XG	脆弱性なし	脆弱性なし
12.2XH	脆弱性なし	脆弱性なし
12.2XI	脆弱性なし	脆弱性なし
12.2XJ	脆弱性なし	脆弱性なし
12.2XK	脆弱性なし	脆弱性なし

12.2XL	脆弱性なし	脆弱性なし
12.2XM	脆弱性なし	脆弱性なし
12.2XN	脆弱性なし	脆弱性なし
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	脆弱性なし	12.2(54)XOより前のリリースには脆弱性があり、12.2(54)XO以降のリリースには脆弱性はありません。
12.2XQ	脆弱性なし	脆弱性なし
12.2XR	脆弱性なし	脆弱性なし
12.2XS	脆弱性なし	脆弱性なし
12.2XT	脆弱性なし	脆弱性なし
12.2XU	脆弱性なし	脆弱性なし
12.2XV	脆弱性なし	脆弱性なし
12.2XW	脆弱性なし	脆弱性なし
12.2YA	12.2(4)YA8より前のリリースには脆弱性があり、12.2(4)YA8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	脆弱性あり。最初の修正はリリース12.4
12.2YB	脆弱性なし	脆弱性なし
12.2YC	脆弱性なし	脆弱性なし

12.2YD	脆弱性なし	脆弱性なし
12.2YE	脆弱性なし	脆弱性なし
12.2YF	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。
12.2YG	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。
12.2YH	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。
12.2YJ	12.2(8)YJ1より前のリリースには脆弱性があり、12.2(8)YJ1以	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

	降のリリースには脆弱性はありません。	ポート組織にお問い合わせください。
12.2YK	脆弱性なし	脆弱性なし
12.2YL	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。
12.2YM	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12.4
12.2YN	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	脆弱性なし	脆弱性なし
12.2YP	脆弱性なし	脆弱性なし

12.2YQ	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。
12.2YR	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。
12.2YS	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。
12.2YT	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。
12.2YU	脆弱性が存在します。このアド	脆弱性が存在します。このアドバイザリの「修正済み

	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。	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。
12.2YV	12.2(11)YV1より前のリリースには脆弱性があり、12.2(11)YV1以降のリリースには脆弱性はありません。	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	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。

	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	脆弱性あり。最初の修正はリリース12.2SXF	脆弱性あり。最初の修正はリリース12.2SXF
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	脆弱性なし	脆弱性なし
12.2ZD	脆弱性なし	脆弱性なし
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12.4
12.2ZF	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12.4
12.2ZG	脆弱性なし	脆弱性なし
12.2ZH	12.2(13)ZH6より前のリリースには脆弱性があり、12.2(13)ZH6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	脆弱性あり。最初の修正はリリース12.4
12.2ZJ	脆弱性なし	脆弱性なし
12.2ZL	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	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。

	い。	
12.2ZP	脆弱性なし	脆弱性なし
12.2ZU	脆弱性あり。最初の修正はリリース12.2SXH	脆弱性あり。最初の修正はリリース12.2SXH
12.2ZX	脆弱性なし	脆弱性なし
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）	2011年9月の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12.4
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12.4
12.3BC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCC
12.3BW	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12.4
12.3JA	脆弱性なし	脆弱性なし
12.3JEA	脆弱性なし	脆弱性なし
12.3JEB	脆弱性なし	脆弱性なし
12.3JEC	脆弱性なし	脆弱性なし
12.3JED	脆弱性なし	脆弱性なし
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以降のリリースには脆弱性はありません。最初の修正はリリース	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

	12.4	
12.3JL	脆弱性なし	脆弱性なし
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12.4
12.3TPC	12.3(4)TPC11aまでのリリースには脆弱性はありません。	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	12.3(2)XA7より前のリリースには脆弱性があり、12.3(2)XA7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	脆弱性あり。最初の修正はリリース12.4
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	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。

	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12.4
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12.4
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12.4
12.3XF	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。
12.3XG	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12.4
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12.2SB
12.3XJ	脆弱性が存在し	脆弱性が存在します。この

	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。	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。
12.3XK	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12.4
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12.4T
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12.4
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12.4
12.3XS	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
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	脆弱性が存在します。このアドバイザリの「修	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

	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。	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。
12.3XX	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12.4
12.3XY	脆弱性なし	脆弱性なし
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12.4
12.3YA	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3YD	脆弱性なし	脆弱性なし
12.3YF	脆弱性なし	脆弱性なし
12.3YG	脆弱性なし	脆弱性なし
12.3YH	脆弱性なし	脆弱性なし
12.3YI	脆弱性なし	脆弱性なし
12.3YJ	脆弱性あり。最初の修正はリリ	脆弱性あり。最初の修正はリリース12.4T

	ース12.4T	
12.3YK	脆弱性なし	脆弱性なし
12.3YM	脆弱性なし	脆弱性なし
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12.4T
12.3YS	脆弱性あり。最初の修正はリリース12.4T 12.3(11)YS1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12.4T
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12.4T
12.3YU	脆弱性あり。最初の修正はリリース12.4XB	脆弱性あり。最初の修正はリリース12.4XB
12.3YX	脆弱性あり。12.4XR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12.4T
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	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

	エアの取得」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。	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12.4T
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2011年9月の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(25e)	12.4(25f)
12.4GC	12.4(24)GC4	12.4(24)GC4
12.4JA	脆弱性なし	脆弱性なし
12.4JAX	脆弱性なし	脆弱性なし
12.4JDA	脆弱性なし	脆弱性なし
12.4JDC	脆弱性なし	脆弱性なし
12.4JHA	脆弱性なし	脆弱性なし
12.4JHB	脆弱性なし	脆弱性なし
12.4JHC	脆弱性なし	脆弱性なし

12.4JK	脆弱性なし	脆弱性なし
12.4JL	脆弱性なし	脆弱性なし
12.4JMA	脆弱性なし	脆弱性なし
12.4JMB	脆弱性なし	脆弱性なし
12.4JX	脆弱性なし	脆弱性あり。12.4JAの任意のリリースに移行 12.4(21a)JXまでのリリースには脆弱性はありません。
12.4JY	脆弱性なし	脆弱性なし
12.4MD	脆弱性なし	12.4(24)MD6（2011年10月28日）
12.4MDA	脆弱性なし	12.4(24)MDA7
12.4MDB	脆弱性なし	12.4(24)MDB3
12.4MR	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。
1240万	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。
12.4MRB	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4SW	脆弱性なし	脆弱性なし
12.4T	12.4(15)T15 12.4(24)T5	12.4(15)T16 12.4(24)T6
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12.4T
12.4XB	12.4(2)XB12	12.4(2)XB12
12.4XC	脆弱性なし	脆弱性なし
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12.4T
12.4XE	脆弱性なし	脆弱性なし
12.4XF	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
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12.4T

12.4XJ	脆弱性なし	脆弱性なし
12.4XK	脆弱性なし	脆弱性なし
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	12.4(15)XMまでのリリースには脆弱性はありません。 12.4(15)XM3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12.4T	脆弱性あり。最初の修正はリリース12.4T
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	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XR	脆弱性なし	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12.4T
12.4XV	脆弱性なし	脆弱性なし
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12.4T
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12.4T
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12.4T

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12.4T
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。
12.4YE	脆弱性なし	脆弱性あり。2011年9月30日に12.4(22)YE6で修正済み。2011年10月17日に12.4(24)YE7で入手可能
12.4YG	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。
影響を受ける 15.0 ベ	First Fixed Release (修正された最初のリ	2011年9月の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

ースのリリース	リース)	リリース
15.0M	15.0(1)M4 15.0(1)M5a	15.0(1)M7
15.0MR	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。
15.0MRA	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。
15.0秒	15.0(1)S3a 15.0(1)S4 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)S4 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。

15.0SE	脆弱性なし	脆弱性なし
15.0SG	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。
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 ベースのリリース	First Fixed Release (修正された最初のリリース)	2011年9月の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	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。
15.1GC	脆弱性なし	脆弱性あり(最初の修正はリリース15.1T)

1,510万	脆弱性なし	15.1(4)M2（2011年9月30日に入手可能）
15.1MR	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。
15.1S	15.1(1)S1 15.1(2)S 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(2)S2 15.1(3)S 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。
15.1T	15.1(1)T3 15.1(2)T2 15.1(3)T	2011年12月9日の15.1(1)T4 15.1(2)T4 15.1(3)T2
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）	2011年9月の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
該当する15.2ベースのリリースはありません		

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リリース	First Fixed Release（修正された最初のリリース）	2011年9月の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	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.2.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.3.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.4.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.5.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.6.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
3.1.xS	3.1.3S	脆弱性あり、3.3.2S以降に移行
3.1.xSG	脆弱性なし	脆弱性あり、3.2.0SG以降に移行
3.2.xS	3.2.1S	脆弱性あり、3.3.2S以

		降に移行
3.2.xSG	脆弱性なし	脆弱性なし
3.3.xS	脆弱性なし	3.3.2S
3.4.xS	脆弱性なし	脆弱性なし

Cisco IOSリリースへのCisco IOS XE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、2011年9月の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 PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、{insert info here}によってシスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw

改訂履歴

リビジョン 1.1	2011年 9月30日	IOSソフトウェアテーブルバンドル公開のアップデートの最初の修正済み情報。

リビジョン 1.0	2011年 9月28日	初回公開リリース

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。