Cisco IOSソフトウェアのネットワークアドレス変換の脆弱性

アドバイザリーID : cisco-sa-20110928-nat
初公開日 : 2011-09-28 16:00
最終更新日 : 2012-09-21 19:21
バージョン 1.4 : Final
回避策 : No Workarounds available
Cisco バグ ID : CSCtd10712 CSCth11006 CSCti98219 CSCso02147 CSCtj04672 CSCti48483

CVE-2011-3280 CVE-2011-3278 CVE-2011-3279 CVE-2011-3276 CVE-2011-3277

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ソフトウェアのネットワークアドレス変換(NAT)機能には、次のプロトコルの変換に関する複数のサービス拒否(DoS)の脆弱性があります。

- NetMeetingディレクトリ(Lightweight Directory Access Protocol、LDAP)
- セッション開始プロトコル.（複数の脆弱性）
- H.323プロトコル

このドキュメントで説明されているすべての脆弱性は、該当するデバイス上で転送中のパケットでアプリケーション層の変換が必要になることにより発生します。

シスコはこれら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。

本アドバイザリは以下にて確認可能です。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

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

Cisco IOSソフトウェアを実行しているシスコデバイスは、NATが設定されており、次の機能の1つ以上のサポートが含まれている場合に脆弱性が存在します。

- NetMeetingディレクトリNAT（TCPポート389のLDAP）
- セッション開始プロトコル(SIP)用のNAT
- H.323用NAT

Cisco IOSデバイスでNATが有効になっているかどうかを確認するには、デバイスにログインして、show ip nat statisticsコマンドを発行することを推奨します。NATがアクティブな場合、Outside interfacesとInside interfacesのセクションにはそれぞれ少なくとも1つのインターフェイスが含まれます。次の例は、NAT機能がアクティブになっているデバイスを示しています。

```
<#root>

Router#

show ip nat statistics


Total translations: 2 (0 static, 2 dynamic; 0 extended)

Outside interfaces: Serial0
Inside interfaces: Ethernet1

Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool mypool refcount 2
 pool mypool: netmask 255.255.255.0
        start 192.168.10.1 end 192.168.10.254
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

Cisco IOSソフトウェアリリースによっては、Outside interfacesおよびInside interfacesの行に続く行にインターフェイスリストが表示される場合があります。showコマンドのsectionフィルタをサポートしているリリースでは、管理者はshow ip nat statistics | section interfacesコマンドを使用します。

```
<#root>

Router>

show ip nat statistics | section interfaces

Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Router>
```

また、Cisco IOSソフトウェアの設定でNATが有効になっているかどうかを判断するには、ip nat insideコマンドとip nat outsideコマンドがそれぞれ別のインターフェイスに存在している必要があります。NAT仮想インターフェイスの場合は、ip nat enableインターフェイスコマンドが存在します。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインして show version コマンドを使って、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、シスコ製品がCisco IOSソフトウェアリリース15.0(1)M1を実行し、インストールされているイメージ名がC3900-UNIVERSALK9-Mであることを示しています。

```
<#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


!--- output truncated
```

Cisco IOSソフトウェアのリリース命名規則の追加情報は、『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

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

NAT for NetMeeting Directory(LDAP)の脆弱性

LDAPは、IPネットワークに実装されたディレクトリサービスのデータを照会および変更するためのプロトコルです。NetMeeting Directory用のNAT(Internet Locator Service(ILS)とも呼ばれる)は、TCPポート389でLDAPパケットを変換します。検査されたポートは設定できません。

この脆弱性は、NetMeetingディレクトリのNAT機能で処理する必要がある不正なトランジットLDAPトラフィックによって引き起こされます。

この脆弱性は、Cisco Bug ID CSCtd10712(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-2011-0946が割り当てられています。

SIP DoS脆弱性に対するNAT

このドキュメントでは、SIPに対するNAT機能における4つの脆弱性について説明します。

SIP over TCPに対するNATの脆弱性:TCPポート5060で巧妙に細工されたSIPパケットが原因で、脆弱性のあるデバイスのリロードなど、予期しない結果が発生する可能性があります。この脆弱性の修正により、SIP over TCPパケットの変換はデフォルトで無効になります。この脆弱性は、Cisco Bug ID CSCso02147(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)CVE-2011-3276が割り当てられています。

Provider edge Multiprotocol Label Switching(MPLS)NAT of SIP over UDP packets DoS vulnerability:UDP 5060上の不正なSIPパケットがMPLS対応の脆弱なデバイスを通過する際に、不正なパケットにMPLSタグを付加する必要がある場合、デバイスがリロードされる可能性があります。この脆弱性は、Cisco Bug ID CSCti98219(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2011-3279が割り当てられています。

巧妙に細工されたSIP over UDPパケットに対するNATのDoS脆弱性:SIP変換を必要とするUDPポート5060での同様の巧妙に細工されたパケットに関連して、2つのDoS脆弱性があります。1つ目はデバイスのリロードを引き起こす脆弱性で、2つ目は脆弱性のあるデバイスのリロードなど、DoS状態を引引きききき起こす可能性があるがあるメモリリークのを原因原因です。SIPのNATの脆弱性は、Cisco Bug ID CSCti48483(登録ユーザ専用)およびCisco Bug ID CSCtj04672(登録ユーザ専用)に記載されています。CVE IDとしてCVE-2011-3278とCVE-2011-3280が割り当てられています。

H.323パケットのNATにおけるDoS脆弱性

巧妙に細工されたH.323パケットがTCPポート1720を通過すると、脆弱性のあるデバイスが再起動する可能性があります。この脆弱性は、Cisco Bug ID CSCth11006(登録ユーザ専用) (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-

3277が割り当てられています。

回避策

IPパケットのペイロードに埋め込まれたIPアドレスの変換を無効にすることで、このアドバイザリに記載されている脆弱性を緩和できます。異なるプロトコルに対してNATを無効にするには、異なる設定が必要です。一部のプロトコルでは、1つのコマンドを使用できます。その他のプロトコルでは、個々のNAT変換ルールを設定に追加する必要があります。

NAT LDAPの脆弱性の緩和

LDAPのNATを無効にするには、no-payloadキーワードを使用してLDAPインスペクションを無効にするようにポートベースのアドレス変換を設定する必要があります。これにより、レイヤ3（ポート固有ではない）でのLDAPパケットのNATは引き続き許可されます。他の非LDAPプロトコルの変換は影響を受けません。NetMeeting Directoryなど、LDAPに埋め込まれたIPアドレスを使用するアプリケーションは、埋め込まれたIPアドレスを変換する必要がある場合に悪影響を受けます。

次に、2つのNATルールに対する緩和策を含む設定例を示します。

```
<#root>

!-- NAT rule for port TCP/389 to disable IP NAT for LDAP translation
!-- Takes precedence over the non-port translation rule.

ip nat outside source static tcp 192.168.0.1 389 192.168.1.1 389 no-payload

ip nat outside source static tcp 192.168.0.3 389 192.168.1.3 389 no-payload

!-- Translation rule for all other protocols

ip nat outside source static 192.168.0.1 192.168.1.1
ip nat outside source static 192.168.0.3 192.168.1.3

interface GigabitEthernet0/0
  ip nat inside

interface GigabitEthernet0/1
  ip nat outside
```

設定内の各NAT変換ルールを更新して、ポート389でのTCPパケットの変換を無効にするポートごとのルールを追加する必要があります。

SIP over TCPに対するNATのDoS脆弱性の緩和

この脆弱性に対する緩和策は、no ip nat service sip tcp port 5060グローバルコンフィギュレーションコマンドを使用して、SIP over TCPトランスポートに対するNATを無効にすることです。

巧妙に細工されたSIP over UDPパケットに対するNATによるDoS脆弱性の緩和

これらの脆弱性を緩和するには、no ip nat service sip udp port 5060グローバルコンフィギュレーションコマンドを使用して、SIP over UDPトランスポートに対してNATを無効にします。

巧妙に細工されたH.323パケットに対するNATによるDoS脆弱性の緩和

この脆弱性に対する緩和策は、no ip nat service h225グローバルコンフィギュレーションコマンドを使用して、H.323およびH.225.0に対してNATを無効にすることです。

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、https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.xのCisco Security(SIO)ポータルでも入手できます。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	First Fixed	2011年9月のバンドル

12.0-Based Releases	Release（修正された最初のリリース）	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-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
12.1E	脆弱性なし	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	脆弱性あり。最初の修正はリリース12.4
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	脆弱性あり。最初の修正はリリース12.2SB

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
12.2CY	脆弱性なし	脆弱性なし
12.2CZ	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
12.2DA	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	脆弱性あり。最初の修正はリリース12.2SG 12.2(20)EW4までのリリースには脆弱性はありません。	12.2(20)EW4までのリリースには脆弱性はありません。
12.2EWA	脆弱性あり。最初の修正はリリース12.2SG	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	12.2(55)EX	12.2(55)EX3
12.2EY	12.2(52)EY 12.2(52)EY1b	12.2(58)EY
12.2EZ	脆弱性あり。 15.0SEの任意のリリースに移行	脆弱性あり。 15.0SEの任意のリリースに移行
12.2FX	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12.2SE)
12.2FY	脆弱性あり(最初の修正はリリース12.2EX)	脆弱性あり(最初の修正はリリース12.2EX)
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「	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。
12.2IXD	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
12.2MRB	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。
12.2S	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)SCE1
12.2SCF	脆弱性なし	脆弱性なし
12.2SE	12.2(55)SE2 12.2(58)SE	12.2(55)SE3 12.2(58)SE
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12.2SE)
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12.2SE)

12.2秒	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12.2SE)
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12.2SE)
12.2参照	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12.2SE)
12.2SEF	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12.2SE)
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12.2EX	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(53)SG4	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	脆弱性あり。最初の修正はリリース12.2SG	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	脆弱性なし	脆弱性なし
12.2SQ	12.2(50)SQ3	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(29b)SV1より前のリリースには脆弱性があり、12.2(29b)SV1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	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。
12.2SX	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
12.2SXF	12.2(18)SXF17b	12.2(18)SXF17b
12.2SXH	脆弱性あり。最初の修正はリリース12.2SXI	脆弱性あり。最初の修正はリリース12.2SXI
12.2SXI	12.2(33)SXI6	12.2(33)SXI6
12.2日本語	12.2(33)SXJ1	12.2(33)SXJ1
12.2SY	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。
12.2SZ	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。
12.2XA	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	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。最初の修正はリリース12.2SG	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	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
12.2YB	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。
12.2YH	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	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。
12.2年	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。
12.2YR	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。
12.2YS	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。
12.2YV	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。
12.2年	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	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。
12.2YY	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	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
12.2ZJ	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。	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。
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
12.3BW	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12.4	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
12.3JL	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	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	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。
12.3XC	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。

12.3XK	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
12.3XU	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。
12.3XX	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
12.3YD	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。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.3年	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	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。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
12.3YZ	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(25f)	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。	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	12.4(24)MD6（10月11日）	12.4(24)MD6（10月11日）
12.4MDA	12.4(24)MDA7	12.4(24)MDA7
12.4MDB	12.4(24)MDB3	12.4(24)MDB3
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	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。
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12.4T
12.4SW	脆弱性なし	脆弱性なし
12.4T	12.4(15)T16 12.4(24)T6	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	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
12.4XN	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12.4T
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	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。	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(22)YE6（2011年9月30日に入手可能） 12.4(24)YE7（10月17日に入手可能）	12.4(22)YE6（2011年9月30日に入手可能） 12.4(24)YE7（10月17日に入手可能）
12.4YG	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。
該当する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）	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
15.0M	15.0(1)M7	15.0(1)M7
15.0MR	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。
15.0MRA	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	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。	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)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。
15.0SE	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	15.1(2)EY	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)
1,510万	15.1(4)M2（2011年9月30日に入手可能）	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(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。	15.1(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)T4（2011年12月9日に入手可能） 15.1(2)T4 15.1(3)T2	15.1(1)T4（2011年12月9日に入手可能） 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)
影響を受ける15.2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
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	脆弱性なし	脆弱性あり、3.3.2S以降に移行
3.1.xSG	脆弱性あり、3.2.0SG以降に移行	脆弱性あり、3.2.0SG以降に移行
3.2.xS	脆弱性なし	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

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

NAT LDAPの脆弱性および巧妙に細工されたSIPパケットに対するNATの脆弱性は、シスコ内部でのテストによって発見されました。NAT SIP/TCPの脆弱性、SIP over UDPパケットのプロバイダーエッジMPLS NATの脆弱性、およびH.323パケットのNATのDoSの脆弱性は、TAC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-20110928-nat

改訂履歴

リビジョン 1.4	2012年5月14日	12.1Eの脆弱性ステータスを更新します。
リビジョン 1.3	2012年2月17日	Cisco IOS 12.2SXHに関するCisco IOSソフトウェアテーブルの情報を更新。
リビジョン 1.2	2011-Oct-21	CSCtd10712に関するバックエンド情報を修正。セキュリティアドバイザリ自体に変更はありません。
リビジョン 1.1	2011年9月30日	リリース12.2MRB、12.2SXH、12.2SXI、12.2SXJ、および12.2SYの修正済みCisco IOSソフトウェアテーブルの情報を更新。
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。