Cisco IOS Software Zone-Based Policy Firewall Session Initiation Protocol Inspection Denial of Service Vulnerability

Advisory ID: cisco-sa-20130327-cce

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-cce/

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

Revision 1.1

Last Updated 2013 April 11 15:36 UTC (GMT)

For Public Release 2013 March 27 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアには、不正な Session Initiation Protocol (SIP; セッション開始プロトコル) メッセージの処理により引き起こされる、メモリ リークの脆弱性が存在します。この脆弱性が不正利用されると、サービスの中断が引き起こされる可能性があります。この脆弱性の影響を受けるのは、SIP インスペクションが設定されているデバイスだけです。

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。SIP インスペクションを実行する必要のあるデバイスについては回避策がありません。

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-20130327-cce/

注：2013 年 3 月 27 日の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には、7 件のセキュリティ アドバイザリが含まれています。これらのアドバイザリはすべて、Cisco IOS ソフトウェアの脆弱性に対処するものです。各 Cisco IOS ソフトウェア セキュリティ 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修正する Cisco IOS ソフトウェア リリース、および 2013 年 3 月にバンドル公開したすべての Cisco IOS ソフトウェアの脆弱性を修正する Cisco IOS ソフトウェア リリースを記載しています。

個別の公開リンクは、次のリンクにある「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

該当製品

脆弱性が認められる製品

該当する Cisco IOS ソフトウェア バージョンが稼働しているシスコ デバイスの Zone-Based Policy Firewall（ZBFW）下で、Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）インスペクションが設定されている場合、この脆弱性の影響を受けます。

デバイスの Zone-Based Policy Firewall（ZBFW）下で Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）インスペクションが設定されているかどうかを確認するには、 **show policy-map type inspect zone-pair | include sip** 特権 EXEC コマンドを実行して、出力に **Match: protocol sip** が含まれるかどうかを確認します。Zone-Based Policy Firewall（ZBFW）下で Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）インスペクションが有効にされている Cisco IOS ソフトウェアを稼働するデバイスで、**show policy-map type inspect zone-pair | include sip** コマンドを実行した結果の出力を次に示します。

```
Cisco#show policy-map type inspect zone-pair | include sip
Match: protocol sip
```

デフォルトでは SIP トラフィックのインスペクションは有効になっていません。

SIP トラフィックのネットワーク アドレス変換（NAT）はこの脆弱性の影響を受けません。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインし **show version** コマンドを実行してシステム バナーを表示させます。「Internetwork Operating System Software」、「Cisco IOS Software」あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼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、続いてバージョンと Cisco IOS ソフトウェア リリース名が表示されます。他のシスコ デバイスでは、**show version** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.0(1)M1 が稼働し、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。

```
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_teamRouter> 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以下のリンクにある「White Paper: Cisco IOS and NX-OS Software Reference Guide」で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性が認められない製品

Cisco IOS XR ソフトウェアは、この脆弱性の影響を受けません。

Cisco IOS XE ソフトウェアは、この脆弱性の影響を受けません。

この脆弱性の影響を受ける他のシスコ製品は、現在確認されていません。

詳細

Session Initiation Protocol（SIP; セッション開始プロトコル）インスペクションは Cisco IOS ファイアウォール機能であり、基本的な SIP ディープ パケット インスペクション機能（SIP パケット インスペクションとピンホール オープニング）ならびにプロトコルの遵守とアプリケーション セキュリティの機能を提供します。

Cisco IOS ソフトウェアの Zone-based Policy Firewall（ZBFW）下における Session Initiation Protocol（SIP）インスペクション機能の脆弱性によって、認証されていないリモートの攻撃者がメモリ リークを引き起こし、最終的にデバイスのリロードを発生させる可能性があります。

この脆弱性は、不正な SIP パケットの不適切な処理に起因します。攻撃者はデバイスを通して不正な SIP メッセージを送信することで、この脆弱性を不正利用できる可能性があります。この不正利用によって、Cisco IOS ソフトウェアが割り当てられたメモリを解放できなくなり、メモリ リークが発生することがあります。攻撃が継続すると、デバイスのリロードが引き起こされる可能性があります。

SIP トラフィックは UDP ポート 5060 と TCP ポート 5060 および 5061 を使用できます。

SIP トラフィックのネットワーク アドレス変換（NAT）はこの脆弱性の影響を受けません。

注：この脆弱性は通過トラフィックによってのみ引き起こされます。該当デバイス宛ての SIP トラフィックはこの脆弱性を引き起こしません。

この脆弱性は、Cisco Bug ID CSCtl99174（ 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-2013-1145 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ 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。

シスコでは、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知ることができます。

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

またシスコでは、各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/

CSCtl99174-- IOSFW: Chunk leaks under certain conditions for malformed SIP packets Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.1**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Official-Fix		Confirmed	

影響

この脆弱性が不正利用されると、該当するデバイスでメモリ リークが引き起こされる可能性があります。この脆弱性が繰り返し不正利用されると、該当するデバイスのリロードが引き起こされ、サービス拒否（DoS）状態が発生するおそれがあります。

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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

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性を含む場合、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 2013 Bundled Publication」列は、Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開に記載されたすべての脆弱性を修正する最初のリリースを示します。可能な限り、最新のリリースにアップグレードすることを推奨します。

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）ポータルで利用できます。
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 2013 Bundled Publication
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2013 Bundled Publication
12.2	Not vulnerable	Not vulnerable
12.2B	Not vulnerable	Not vulnerable
12.2BC	Not vulnerable	Not vulnerable
12.2BW	Not vulnerable	Not vulnerable
12.2BX	Not vulnerable	Not vulnerable
12.2BY	Not vulnerable	Not vulnerable
12.2BZ	Not vulnerable	Not vulnerable
12.2CX	Not vulnerable	Not vulnerable
12.2CY	Not vulnerable	Not vulnerable
12.2CZ	Not vulnerable	Not vulnerable
12.2DA	Not vulnerable	Not vulnerable
12.2DD	Not vulnerable	Not vulnerable
12.2DX	Not vulnerable	Not vulnerable
12.2EU	Not vulnerable	Not vulnerable
12.2EW	Not vulnerable	Vulnerable; First fixed in Release 12.2SG Releases up to and including 12.2(20)EW4 are not vulnerable.
12.2EWA	Not vulnerable	Vulnerable; First fixed in Release 12.2SG

		Releases up to and including 12.2(20)EWA4 are not vulnerable.
12.2EX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(37)EX are not vulnerable.
12.2EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
12.2EZ	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FY	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FZ	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2IRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXA	Not vulnerable	Not vulnerable
12.2IXB	Not vulnerable	Not vulnerable
12.2IXC	Not vulnerable	Not vulnerable
12.2IXD	Not vulnerable	Not vulnerable
12.2IXE	Not vulnerable	Not vulnerable
12.2IXF	Not vulnerable	Not vulnerable
12.2IXG	Not vulnerable	Not vulnerable
12.2IXH	Not vulnerable	Not vulnerable
12.2JA	Not vulnerable	Not vulnerable
12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Not vulnerable
12.2MC	Not vulnerable	Not vulnerable
12.2MRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2S	Not vulnerable	Vulnerable.Only releases 12.2(25)S through 12.2(25)S15 are vulnerable
12.2SB	Not vulnerable	12.2(33)SB12
12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2SCA	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCB	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCC	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCD	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCE	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCF	Not vulnerable	12.2(33)SCF4
12.2SCG	Not vulnerable	Not vulnerable
12.2SCH	Not vulnerable	Not vulnerable

12.2SE	Not vulnerable	12.2(55)SE7 Releases up to and including 12.2(54)SE4 are not vulnerable.
12.2SEA	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEB	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEC	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SED	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEE	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEF	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEG	Not vulnerable	Releases prior to 12.2(25)SEG4 are vulnerable; Releases 12.2(25)SEG4 and later are not vulnerable.First fixed inRelease 15.0SE
12.2SG	Not vulnerable	12.2(53)SG9
12.2SGA	Not vulnerable	Vulnerable; First fixed in Release 12.2SG
12.2SM	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SO	Not vulnerable	Not vulnerable
12.2SQ	Not vulnerable	12.2(50)SQ5
12.2SRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	Not vulnerable	12.2(33)SRE8
12.2STE	Not vulnerable	Not vulnerable
12.2SU	Not vulnerable	Not vulnerable
12.2SV	Not vulnerable	Vulnerable.Only releases 12.2(25)SV2, 12.2(27)SV5 and 12.2(29)SV3 are vulnerable.
12.2SVA	Not vulnerable	Not vulnerable
12.2SVC	Not vulnerable	Not vulnerable
12.2SVD	Not vulnerable	Not vulnerable
12.2SVE	Not vulnerable	Not vulnerable
12.2SW	Not vulnerable	Vulnerable; First fixed in Release 15.0M * Releases up to and including 12.2(23)SW1 are not vulnerable.
12.2SX	Not vulnerable	Not vulnerable
12.2SXA	Not vulnerable	Not vulnerable
12.2SXB	Not vulnerable	Not vulnerable
12.2SXD	Not vulnerable	Not vulnerable
12.2SXE	Not vulnerable	Not vulnerable
12.2SXF	Not vulnerable	Not vulnerable
12.2SXH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXI	Not vulnerable	12.2(33)SXI11
12.2SXJ	Not vulnerable	12.2(33)SXJ5
12.2SY	Not vulnerable	12.2(50)SY4
12.2SZ	Not vulnerable	Not vulnerable
12.2T	Not vulnerable	Not vulnerable
12.2TPC	Not vulnerable	Not vulnerable
12.2WO	Not vulnerable	Not vulnerable
12.2XA	Not vulnerable	Not vulnerable
12.2XB	Not vulnerable	Not vulnerable

12.2XC	Not vulnerable	Not vulnerable
12.2XD	Not vulnerable	Not vulnerable
12.2XE	Not vulnerable	Not vulnerable
12.2XF	Not vulnerable	Not vulnerable
12.2XG	Not vulnerable	Not vulnerable
12.2XH	Not vulnerable	Not vulnerable
12.2XI	Not vulnerable	Not vulnerable
12.2XJ	Not vulnerable	Not vulnerable
12.2XK	Not vulnerable	Not vulnerable
12.2XL	Not vulnerable	Not vulnerable
12.2XM	Not vulnerable	Not vulnerable
12.2XNA	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNB	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNC	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XND	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNE	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNF	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XO	Not vulnerable	Releases prior to 12.2(54)XO are vulnerable; Releases 12.2(54)XO and later are not vulnerable.First fixed inRelease 12.2SG
12.2XQ	Not vulnerable	Not vulnerable
12.2XR	Not vulnerable	Not vulnerable
12.2XS	Not vulnerable	Not vulnerable
12.2XT	Not vulnerable	Not vulnerable
12.2XU	Not vulnerable	Not vulnerable
12.2XV	Not vulnerable	Not vulnerable
12.2XW	Not vulnerable	Not vulnerable
12.2YA	Not vulnerable	Not vulnerable
12.2YC	Not vulnerable	Not vulnerable
12.2YD	Not vulnerable	Not vulnerable
12.2YE	Not vulnerable	Not vulnerable
12.2YK	Not vulnerable	Not vulnerable
12.2YO	Not vulnerable	Not vulnerable
12.2YP	Not vulnerable	Not vulnerable
12.2YT	Not vulnerable	Not vulnerable
12.2YW	Not vulnerable	Not vulnerable
12.2YX	Not vulnerable	Not vulnerable
12.2YY	Not vulnerable	Not vulnerable
12.2YZ	Not vulnerable	Not vulnerable
12.2ZA	Not vulnerable	Not vulnerable
12.2ZB	Not vulnerable	Not vulnerable
12.2ZC	Not vulnerable	Not vulnerable
12.2ZD	Not vulnerable	Not vulnerable
12.2ZE	Not vulnerable	Not vulnerable
12.2ZH	Not vulnerable	Not vulnerable
12.2ZJ	Not vulnerable	Not vulnerable
12.2ZP	Not vulnerable	Not vulnerable
12.2ZU	Not vulnerable	Not vulnerable

12.2ZX	Not vulnerable	Not vulnerable
12.2ZY	Not vulnerable	Not vulnerable
12.2ZYA	Not vulnerable	Not vulnerable
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**
12.4	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4GC	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	Not vulnerable
12.4JAL	Not vulnerable	Not vulnerable
12.4JAM	Not vulnerable	Releases prior to 12.4(25e)JAM are vulnerable; Releases 12.4(25e)JAM and later are not vulnerable.Migrate to any release in 12.4JAN12.4(25e)JAM
12.4JAX	Not vulnerable	Not vulnerable
12.4JAZ	Not vulnerable	Not vulnerable
12.4JDA	Not vulnerable	Not vulnerable
12.4JDC	Not vulnerable	Not vulnerable
12.4JDD	Not vulnerable	Not vulnerable
12.4JDE	Not vulnerable	Not vulnerable
12.4JHA	Not vulnerable	Not vulnerable
12.4JHB	Not vulnerable	Not vulnerable
12.4JHC	Not vulnerable	Not vulnerable
12.4JK	Not vulnerable	Not vulnerable
12.4JL	Not vulnerable	Not vulnerable
12.4JX	Not vulnerable	Not vulnerable
12.4JY	Not vulnerable	Not vulnerable
12.4JZ	Not vulnerable	Not vulnerable
12.4MD	Vulnerable; First fixed in Release 12.4MDB Releases up to and including 12.4(15)MD5 are not vulnerable.	Vulnerable; First fixed in Release 12.4MDB
12.4MDA	Vulnerable; First fixed in Release 12.4MDB	Vulnerable; First fixed in Release 12.4MDB
12.4MDB	12.4(24)MDB13	12.4(24)MDB13
12.4MR	Releases up to and including 12.4(19)MR3 are not vulnerable.	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 advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4MRB	Vulnerable; First fixed in Release 15.0M *	Vulnerable; First fixed in Release 15.0M *
12.4SW	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4T	Vulnerable; First fixed in Release 15.0M * Releases up to and including 12.4(15)T17 are not vulnerable.	Vulnerable; First fixed in Release 15.0M *
12.4XA	Not vulnerable	Vulnerable; First fixed in Release 15.0M *

12.4XB	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XC	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XD	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XE	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XF	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XG	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XJ	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XK	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XL	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XM	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XN	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XP	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XQ	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XR	Vulnerable; First fixed in Release 15.0M * Releases up to and including 12.4(15)XR10 are not vulnerable.	Vulnerable; First fixed in Release 15.0M *
12.4XT	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XV	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XW	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XY	Not vulnerable	Vulnerable; First fixed in Release 15.0M *
12.4XZ	Vulnerable; First fixed in Release 15.0M *	Vulnerable; First fixed in Release 15.0M *
12.4YA	Vulnerable; First fixed in Release 15.0M *	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)YE3e	12.4(24)YE3e
12.4YG	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 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**
15.0EB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0ED	Not vulnerable	Not vulnerable
15.0EY	Not vulnerable	Not vulnerable
15.0M	15.0(1)M10 *	15.0(1)M10 *
15.0MR	Not vulnerable	Vulnerable; contact your support organization

		per the instructions in Obtaining Fixed Software section of this advisory.
15.0S	Not vulnerable	Vulnerable; First fixed in Release 15.1S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SE	Not vulnerable	15.0(2)SE1
15.0SG	Not vulnerable	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SQA	Not vulnerable	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	Not vulnerable	15.0(1)SY4
15.0XA	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.0XO	Not vulnerable	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 2013 Bundled Publication**
15.1EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
15.1GC	15.1(4)GC1	15.1(4)GC1
15.1M	15.1(4)M6	15.1(4)M6
15.1MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1S	Not vulnerable	** See footnote Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Not vulnerable	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SVA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SVC	Not vulnerable	Not vulnerable
15.1SY	Not vulnerable	15.1(1)SY1; Available on 24-MAY-13
15.1T	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.1XB	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
Affected 15.2-Based	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**

Releases		
There are no affected 15.2 based releases		
Affected 15.3-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2013 Bundled Publication
There are no affected 15.3 based releases		

* Cisco IOS ソフトウェア リリース 15.0M は、2013 年 4 月 1 日にソフトウェア メンテナンスが終了し、新たなリビルドは行われません。詳細は、 サポート終了のお知らせをご覧ください。Cisco IOS ソフトウェア リリース 15.1M への移行をご検討ください。

† Cisco 7600 シリーズのルータ用の最初の修正リリースは Cisco IOS ソフトウェア リリース 15.1(3)S5 で、2013 年 3 月 の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開に記載されます。Cisco 7200 および 7300 シリーズのルータ用の最初の修正リリースは Cisco IOS ソフトウェア リリース 15.1(3)S5a で、2013 年 3 月 の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開に記載され 2013 年 4 月 15 日に公開を予定しています。

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せん。

Cisco IOS XR ソフトウェア

Cisco IOS XR 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せん。

回避策

SIP トラフィックのインスペクションを無効にするとこの脆弱性を軽減できます。SIP トラフィックのインスペクションを無効にするには、Zone-Based Policy Firewall (ZBFW) 設定で使用した対応するクラス マップから **match protocol sip** コマンドを削除します。次の例は、クラス マップからこのコマンドを削除する方法を示しています。

```
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
```

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の特有の問題をご確認ください。

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

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 Navigator からアップグレード ソフトウェアを入手できます。 http://www.cisco.com/cisco/software/navigator.html

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、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、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に関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象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ことを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの 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 に無償アップグレードをリクエストしてください。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact 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、シスコの通常の社内セキュリティ テストで発見されたものです。

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-20130327-cce/

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 E 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

本アドバイザリに関する今後の更新は 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。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.1	2013-April-11	Updated vulnerability status for 15.0EY and 15.0SG in bundle-wide column.
Revision 1.0	2013-March-27	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サポート、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の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。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。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。