Cisco Security Advisory: Cisco IOS Software Zone-Based Firewall Vulnerabilities

Advisory ID: cisco-sa-20120328-zbfw

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

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

Revision 1.0

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

目次

要約

Cisco IOS ソフトウェアには Cisco IOS Zone-Based Firewall 機能に関連する脆弱性が 4 つ存在します。これらの脆弱性は次のとおりです。

- 巧妙に細工された IP パケットに関連するメモリ リーク
- HTTP インスペクションにおけるメモリ リーク
- H.323 インスペクションにおけるメモリ リーク
- SIP インスペクションにおけるメモリ リーク

これらの脆弱性を軽減する回避策はありません。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。

このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

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

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

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

該当製品

脆弱性が存在する製品

脆弱な Cisco IOS バージョンが稼働する Cisco IOS デバイスは、Cisco IOS Zone-Based Firewall に関する 4 つの脆弱性の影響を受けます。これらの脆弱性は、互いに独立して存在します。影響が生じる設定かどうかについては、次の方法で確認してください。

デバイスに Zone-Based Firewall の設定があるかどうかを確認するには、デバイスにログイン・オ、コマンドライン インターフェイス (CLI) コマンド **show zone security** を実行します。出力のゾーン名にメンバー インターフェイスが示されている場合、そのデバイスは脆弱性の影響を受けます。次の例では、デバイスの GigabitEthernet0/0と GigabitEthernet0/1 の両方に Zone-Based Firewall のルールが設定されています。

```
Router#show zone security
zone self
 Description: System defined zone

zone inside
 Description: *** Inside Network ***
 Member Interfaces:
   GigabitEthernet0/0

zone outside
 Description: *** Outside Network ***
 Member Interfaces:
   GigabitEthernet0/1

Router#
```

次のセクションでは、これらの脆弱性を含む特定の機能に関する詳細を説明します。

巧妙に細工された IP パケットに関連するメモリ リーク

巧妙に細工された IP パケットに関連するメモリ リークの脆弱性は、デバイスに特別な設定が行われているかどうかに関係なく存在します。Zone-Based Firewall が設定されているデバイスはこの脆弱性の影響を受けます。

HTTP インスペクションにおけるメモリ リーク

HTTP インスペクションに関連するメモリ リークの脆弱性の影響を受けるのは、Zone-Based Firewall で HTTP インスペクションを実行するように Zone-Based Firewall が設定されているデバイスです。

デバイスに HTTP インスペクションが設定されているかどうかを判断するには、 **show policy-map type inspect zone-pair | include Match: protocol http** コマンドを実行します。次の例は、Cisco IOS Zone-Based Policy Firewall HTTP インスペクションを設定した脆弱性のあるデバイスを示したものです。

```
Router#show policy-map type inspect zone-pair | include Match: protocol
http
       Match: protocol http
```

H.323 インスペクションにおけるメモリ リーク

H.323 インスペクションに関連するメモリ リークの脆弱性の影響を受けるのは、H.323 インスペクションを実行するように Zone-Based Firewall が設定されているデバイスです。デバイスに H.323 インスペクションが設定されているかどうかを判断するには、 **show policy-map type inspect zone-pair | include Match: protocol h323** コマンドを実行します。出力に「Match: protocol h323」が含まれる場合、このデバイスには脆弱性があります。次の例は、Cisco IOS Zone-Based Policy Firewall H.323 インスペクションを設定した脆弱性のあるデバイスを示したものです。

```
Router# show policy-map type inspect zone-pair | include Match: protocol
h323
        Match: protocol h323
```

SIP インスペクションにおけるメモリ リーク

デバイスにレイヤ 4 またはレイヤ 7 のセッション開始プロトコル（SIP）アプリケーション固有のポリシーが設定されており、かつこれらのポリシーがいずれかのファイアウォール ゾーンに適用されている場合、そのデバイスには脆弱性があります。デバイスに SIP インスペクションが設定されているかどうかを判断するには、 **show policy-map type inspect zone-pair | include Match: protocol sip** コマンドを実行します。出力に「Match: protocol sip」が含まれる場合、このデバイスには脆弱性があります。次の例は、Cisco IOS Zone-Based Policy Firewall SIP インスペクションを設定した脆弱性のあるデバイスを示したものです。

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

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

```
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
```

脆弱性が存在しない製品

次の製品は、脆弱性の影響を受けないことが確認されています。

- Cisco PIX 500 シリーズ ファイアウォール
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Catalyst 6500 シリーズ スイッチおよび 7600 シリーズ ルータ用 Firewall Services Module（FWSM）
- Cisco XR 12000 シリーズ ルータのマルチサービス ブレード（MSB）の Virtual Firewall（VFW）アプリケーション
- Cisco ACE Application Control Engine Module
- レガシーの Cisco IOS Firewall サポートが設定されている Cisco IOS デバイス
- Cisco IOS XR ソフトウェア
- Cisco IOS XE ソフトウェア
- Cisco Catalyst 6500 シリーズ ASA Services Module
- Context-Based Access Control（CBAC）

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

ファイアウォールは、組織のネットワーク資産へのアクセスをコントロールするネットワーク デバイスです。ファイアウォールは通常、ネットワークへのエントランス ポイントに設置されます。Cisco IOS ソフトウェアのセキュリティ機能を使用すると、組織の要件に合わせてファイアウォール ポリシーを設定できます。

このアドバイザリで公開される脆弱性は、Zone-Based Firewall 機能に影響を与えます。Zone-Based Policy Firewall（または Zone-Policy Firewall あるいは ZFW とも呼ばれる）は、旧来のインターフェイスベースのモデルを刷新し、より柔軟で分かりやすいゾーンベースのモデルにファイアウォールの設定を実現します。インターフェイスはゾーンに割り当てられ、インスペクション ポリシーはゾーン間を移動するトラフィックに適用されます。ゾーン間ポリシーは高い柔軟性と細かさを提供するため、異なるインスペクション ポリシーを、同一のルータ インターフェイスに接続された複数のホスト グループに適用することができます。

Zone-Based Firewall についての詳細は、http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html を参照してください。

巧妙に細工された IP パケットに関連するメモリ リーク

Cisco IOS ソフトウェアにおける Zone-Based Firewall の実装には脆弱性が存在します。これにより、認証されていないリモートの攻撃者が、該当デバイスの再起動またはメモリ リークを引･ォ起こし、システムが不安定になることがあります。これらの脆弱性は、Cisco IOS ソフトウェアを実行しているデバイスが、巧妙に細工された IP パケットを処理することによって引き起こされます。デバイスに設定された IP アドレス宛てのトラフィックによってのみ、この脆弱性の不正利

用が可能です。デバイスを通過するトラフィックによって脆弱性が引き起こされることはありません。

この脆弱性は、Cisco Bug ID CSCto89536（ 登録ユーザのみ ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-1310 が割り当てられています。

HTTP インスペクションにおけるメモリ リーク

HTTP インスペクション エンジン機能により、（ポート 80 でのトンネリング、認証されていないリクエストのメソッド、HTTP 非準拠のファイル転送など）セキュリティ ポリシーの設定により許可されていない HTTP 接続の検知、フィルタができるように Cisco IOS Firewall を設定することが可能になります。

Cisco IOS ソフトウェア HTTP インスペクション機能の実装には脆弱性が存在します。これにより、認証されていないリモートの攻撃者によって該当デバイスの再起動またはメモリ リークが引き起こされ、システムが不安定になることがあります。この脆弱性は、Cisco IOS ソフトウェアを実行しているデバイスが特定の HTTP メッセージを処理することによって引き起こされます。通過 HTTP トラフィックによってこの脆弱性が不正利用されることはありません。

この脆弱性は、Cisco Bug ID CSCtq36153（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2012-0387 が割り当てられています。

HTTP インスペクションについての情報は、http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_fwapc.html を参照してください。

H.323 インスペクションにおけるメモリ リーク

H.323 は、リアルタイムのマルチメディア通信およびパケットベース（IP）のネットワーク会議の ITU 標準です。Cisco IOS ソフトウェア H.323 インスペクション機能の実装には脆弱性が存在します。これにより、認証されていないリモートの攻撃者によって該当デバイスの再起動またはメモリ リークが引き起こされ、システムが不安定になることがあります。この脆弱性は、Cisco IOS ソフトウェアを実行しているデバイスが不正な H.323 メッセージを処理することによって引き起こされます。通過する H.323 トラフィックによってこの脆弱性が不正利用されることはありません。

この脆弱性は、Cisco Bug ID CSCtq45553（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2012-0388 が割り当てられています。

H.323 インスペクションについての情報は、 http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/15-2mt/fw-h323-v3v4-sup.html を参照してください。

SIP インスペクションにおけるメモリ リーク

SIP は一般的なシグナリング プロトコルであり、インターネットなどの IP ネットワークで音声およびビデオ コールの管理に使用されます。SIP はコールのセットアップと終了に関するすべてを処理します。SIP で処理される最も一般的なセッション タイプは音声とビデオですが、SIP はコールのセットアップと終了を必要とするその他のアプリケーションにも柔軟に対応します。SIP コール シグナリングでは、転送プロトコルとして UDP（ポート番号 5060）、TCP（ポート番号 5060）、または Transport Layer Security（TLS）（TCPポート 5061）を使用します。

Cisco IOS SIP インスペクション機能の実装には脆弱性が存在します。これにより、認証されて

いないリモートの攻撃者によって該当デバイスの再起動またはメモリ リークが引き起こされ、システムが不安定になることがあります。この脆弱性は、Cisco IOS ソフトウェアを実行しているデバイスが巧妙に細工された SIP メッセージを処理することによって引き起こされます。通過する SIP トラフィックによってこの脆弱性が不正利用されることはありません。

この脆弱性は、Cisco Bug ID CSCti46171（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2012-1315 が割り当てられています。

SIP インスペクションについての情報は、
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html を参照してください。

メモリ リークの検出

検出されたメモリ リークを表示するには、次の例に示すように特権 EXEC モードで **show memory debug leaks chunks** コマンドを使用します。

```
Router# show memory debug leaks chunks

Adding blocks for GD... I/O memory Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name Processor memory Address Size Alloc_pc PID
Alloc-Proc Name
4733113C 188 419CB164 129 IP Input FW h225 tpkt
```

上記の例は、プロセス FW h225 tpkt でのメモリ リークを示しています。 **show memory debug leaks** コマンドは、Cisco IOS ソフトウェア バージョン 12.3(8)T1 および 12.2(25)S で導入されました。

注意： **show memory debug** コマンドはすべて、メモリの枯渇が見られた場合にルータのメモリ リークを診断する目的でのみ、お客様のネットワーク上で使用してください。これらのコマンドによって CPU 使用率が高くなり、時間に制約のあるプロトコルのフラッピングを引き起こすことがあります。これらのコマンドはメンテナンス ウィンドウでのみ使用することを推奨します。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリン

クで提供しています。

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

Memory Leak associated with crafted IP 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 - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official Fix		Confirmed	

Memory Leak in HTTP inspection 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 - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official Fix		Confirmed	

Memory Leak in H.323 inspection 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 - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official Fix		Confirmed	

Memory Leak in SIP Inspection

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 - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official Fix		Confirmed	

影響

これらの脆弱性の不正利用に成功した場合、該当デバイスでは再起動が発生することがあります。悪用が繰り返されると、持続的な DoS 状態が発生する可能性があります。

ソフトウェア バージョンおよび修正

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories and Responses アーカイブと、後続のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

Cisco IOS ソフトウェア

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

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

Major Release	Availability of Repaired Releases	
Affected 12.0-Base	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security

d Releases		**Advisory 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 2012 Cisco IOS Software Security Advisory Bundled Publication**
There are no affected 12.2 based releases		
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
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 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.4	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 GC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JA	Not vulnerable	12.4(23c)JA4 12.4(25e)JA
12.4JAX	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JDA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this

		advisory.
12.4JDD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JK	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JL	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JX	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JY	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JZ	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4	12.4(22)MD3; Available	12.4(22)MD3; Available

MD	on 30-MAR-12	on 30-MAR-12
12.4 MDA	12.4(24)MDA11	12.4(24)MDA11
12.4 MDB	12.4(24)MDB5a	12.4(24)MDB5a
12.4 MDC	Not vulnerable	Not vulnerable
12.4 MR	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.
12.4 MRA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4 MRB	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.4 SW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 T	12.4(24)T7 Releases up to and including 12.4(15)T17 are not vulnerable.	12.4(15)T17 12.4(24)T7
12.4 XA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XB	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4 XC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XD	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XE	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XF	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XG	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XJ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XK	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XL	Not vulnerable	Vulnerable; contact your support organization per

		the instructions in Obtaining Fixed Software section of this advisory.
12.4 XM	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XN	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4 XP	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4 XQ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XR	Vulnerable; First fixed in Release 12.4T Releases up to and including 12.4(15)XR10 are not vulnerable.	Vulnerable; First fixed in Release 12.4T
12.4 XT	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XV	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4 XW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XY	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4 XZ	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.4 YA	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.4 YB	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.
12.4 YD	Vulnerable; contact your support organization per the instructions in	Vulnerable; contact your support organization per the instructions in

	Obtaining Fixed Software section of this advisory.	Obtaining Fixed Software section of this advisory.
12.4 YE	12.4(24)YE3d	12.4(24)YE3d
12.4 YG	12.4(24)YG4	12.4(24)YG4
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.0 M	15.0(1)M8	15.0(1)M8
15.0 MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0 MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0 S	Not vulnerable	15.0(1)S5 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0 SA	Not vulnerable	Not vulnerable
15.0 SE	Not vulnerable	15.0(1)SE1
15.0 SG	Not vulnerable	15.0(2)SG2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0 SY	Not vulnerable	15.0(1)SY1
15.0 XA	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
15.0 XO	Not vulnerable	Vulnerable; First fixed in Release 15.0SG Cisco IOS XE devices: Please see Cisco IOS XE Software Availability

Affected 15.1-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication
15.1 EY	Not vulnerable	15.1(2)EY2
15.1 GC	15.1(2)GC2	15.1(2)GC2
15.1 M	15.1(4)M3	15.1(4)M4; Available on 30-MAR-12
15.1 MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1 S	Not vulnerable	15.1(3)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1 SG	Not vulnerable	Not vulnerable
15.1 SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1 SNH	Not vulnerable	Not vulnerable
15.1 T	15.1(3)T3	15.1(3)T3
15.1 XB	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.2 GC	15.2(1)GC2	15.2(1)GC2
15.2 S	Not vulnerable	15.2(1)S1 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability

15.2 T	15.2(1)T2 15.2(2)T 15.2(2)T1	15.2(1)T2 15.2(2)T1 15.2(3)T; Available on 30-MAR-12

* Cisco Catalyst 3550 シリーズ スイッチは Internet Key Exchange（IKE; インターネット キー エクスチェンジ）機能をサポートしており、デバイスがレイヤ 3 イメージを実行しているとき Cisco bug ID CSCts38429 の脆弱性に該当します。ただし、この製品はソフトウェア メンテナンス終了となっています。レイヤ 2 イメージを実行している Cisco 3550 シリーズ SMI スイッチは IKE をサポートしておらず、この脆弱性に該当しません。12.2SE ベースのソフトウェアを稼動しているほかのシスコ デバイスはこの脆弱性に該当しません。

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

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

Cisco IOS XR ソフトウェア

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

回避策

このアドバイザリに記載されている脆弱性に対する回避策はありません。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

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

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Center からアップグレードを入手することができます。 http://www.cisco.com

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、適切な処置について支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策または修正が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC を通して無償アップグレードをお求めください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

これらの脆弱性は、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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

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

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

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

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

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

更新履歴

Revision 1.0	2012-March-28	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。