Cisco IOSソフトウェアゾーンベースファイアウォールの脆弱性

アドバイザリーID : cisco-sa-20120328-zbfw
初公開日 : 2012-03-28 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCtq45553 CSCtq36153 CSCto89536 CSCti46171

CVE-2012-1310
CVE-2012-0388
CVE-2012-1315
CVE-2012-0387

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、Cisco IOS Zone-Based Firewall機能に関連する4つの脆弱性が含まれています。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インスペクションでのメモリリーク
- H.323インスペクションでのメモリリーク
- SIPインスペクションでのメモリリーク

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次のリンクで確認できます。
https://sec.cloudapps.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、このアドバイザリで説明されている脆弱性を修正したCisco IOSソフトウェアリリースと、2012年3月のバンドル公開のすべての脆弱性を修正したCisco IOSソフトウェアリリースが記載されています。

個々の公開リンクは、次のリンクの「Cisco Event Response: Semi-Annual Cisco IOS Software

Security Advisory Bundled Publication」に掲載されています。

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

該当製品

脆弱性のある製品

脆弱性のあるバージョンのCisco IOSソフトウェアを実行しているCisco IOSデバイスは、Cisco IOS Zone-Based Firewallの4つの脆弱性の影響を受けます。これらの脆弱性は相互に関連していません。影響を受ける設定を確認するための詳細を次に示します。

デバイスでゾーンベースファイアウォールが設定され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 zone securityコマンドラインインターフェイス(CLI)コマンドを発行します。出力のゾーン名の下にメンバーインターフェイスが表示されている場合、そのデバイスには脆弱性が存在します。次の例は、GigabitEthernet0/0とGigabitEthernet0/1の両方でゾーンベースファイアウォール規則が設定されたデバイスを示しています。

```
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、脆弱性が含まれている特定の機能の詳細について説明します。

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に対してデバイスが脆弱になるために必要な特別な設定はありません。ゾーンベースファイアウォールが設定されている場合、そのデバイスには脆弱性が存在します。

HTTPインスペクションでのメモリリーク
HTTPインスペクションに関連するメモリリークに対してデバイスが脆弱であるためには、ゾーンベースファイアウォールでHTTPインスペクションを実行するようにゾーンベースファイ

アウォールを設定する必要があります。

デバイスでHTTP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コマンドを入力します。 | include Match: protocol httpコマンドを使用します。次の例は、Cisco IOS Zone-Based Policy Firewall HTTPインスペクションが設定された脆弱性のあるデバイスを示しています。

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

H.323インスペクションでのメモリリーク
H.323検査に関連するメモリリークに対してデバイスが脆弱であるためには、H.323検査を実行するようにゾーンベースファイアウォールを設定する必要があります。デバイスでH.323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コマンドを入力します。 | include Match:protocol h323。出力に「Match: protocol h323」が含まれている場合、そのデバイスには脆弱性が存在します。次の例は、Cisco IOS Zone-Based Policy Firewall H.323インスペクションが設定された脆弱性のあるデバイスを示しています。

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

SIPインスペクションでのメモリリーク
設定にレイヤ4またはレイヤ7のSession Initiation Protocol(SIP)アプリケーション固有のポリシーが設定されており、そのポリシーが任意のファイアウォールゾーンに適用されている場合、デバイスは脆弱になります。デバイスでSIP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コマンドを入力します。 | include Match:protocol sipです。出力に「Match: protocol sip」が含まれている場合、そのデバイスには脆弱性が存在します。次の例は、Cisco IOS Zone-Based Policy Firewall SIPインスペクションが設定された脆弱性のあるデバイスを示しています。

```
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
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、次のリンクの『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を参照。

脆弱性を含んでいないことが確認された製品

次の製品には脆弱性が存在し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シリーズルータ用ファイアウォールサービスモジュール(FWSM)
- Cisco XR 12000シリーズルータのマルチサービスブレード(MSB)上の仮想ファイアウォール(VFW)アプリケーション
- Cisco ACE アプリケーション コントロール エンジン モジュール
- 従来のCisco IOS Firewallサポートが設定された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サービスモジュール
- コンテキストベース アクセス コントロール（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制御するネットワークデバイスです。ファイアウォールは、多くの場合、ネットワークの入り口に配置されます。Cisco IOSソフトウェアは、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るセキュリティ機能のセットを提供します。

このアドバイザリに記載されている脆弱性は、ゾーンベースファイアウォール機能に影響を与えます。ゾーンベースポリシーファイアウォール(またはゾーンポリシーファイアウォール(ZFW)とも呼ばれる)は、以前のインターフェイスベースのモデルから、より柔軟性が高く、わかりやすいゾーンベースのモデルにファイアウォール設定を更新します。インターフェイスはゾーンに割り当てられ、検査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。ゾーン間ポリシーでは十分な柔軟性と精度が提供されるので、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 グループにさまざまな検査ポリシーを適用できます。

ゾーンベースファイアウォールの詳細については、
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ソフトウェアのゾーンベースファイアウォールの実装には脆弱性が存在します。これにより、リモート攻撃者が該当デバイスのリロードを引き起こしたり、システムを不安定にする可能性があるメモリリークを引き起こしたりする可能性があります。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。この脆弱性は、デバイスに設定されたIPアドレスを宛先とするトラフィックによってのみ引き起こされます。通過トラフィックは不正利用の手段とはなりません。

この脆弱性は、Cisco Bug ID CSCto89536(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-2012-1310が割り当てられています。

HTTPインスペクションでのメモリリーク
HTTPインスペクションエンジン機能を使用すると、ユーザはCisco IOSファイアウォールを設定して、セキュリティポリシー設定の範囲内で許可されていないHTTP接続（ポート80を介したトンネリング、未承認の要求方式、HTTP非準拠のファイル転送など）を検出してフィルタリングできます。

Cisco IOSソフトウェアのHTTPインスペクション機能には脆弱性が存在します。この機能を実装すると、リモートの攻撃者によって該当デバイスのリロードが引き起こされたり、システムが不安定になる可能性があるメモリリークが引き起こされたりする可能性があります。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ときに発生します。トランジットHTTPトラフィックは、不正利用の手段となります。

この脆弱性は、Cisco Bug ID CSCtq36153(登録ユーザ専用)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検査の詳細については、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インスペクションでのメモリリーク
H.323は、パケットベース(IP)ネットワークを介したリアルタイムマルチメディア通信および会議のITU標準です。Cisco IOSソフトウェアのH.323インスペクション機能には脆弱性が存在します。この機能を実装すると、リモートの攻撃者によって該当デバイスのリロードが引き起こされたり、システムが不安定になる可能性があるメモリリークが引き起こされたりする可能性があります。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と引き起こされます。通過H.323トラフィックは、不正利用の手段となります。

この脆弱性は、Cisco Bug ID CSCtq45553(登録ユーザ専用)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検査の詳細については、 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インスペクションでのメモリリーク
SIPは、インターネットなどのIPネットワークを介した音声およびビデオコールの管理に使用される一般的なシグナリングプロトコルです。SIPは、コールのセットアップと終了のすべての側面を処理する役割を担います。音声とビデオは、SIPで処理される最も一般的なセッションタイプですが、このプロトコルには、コールのセットアップと終了を必要とする他のアプリケーションに対応できる柔軟性があります。SIPコールシグナリングでは、基本のトランスポートプロトコルとして、UDP（ポート5060）、TCP（ポート5060）、またはTransport Layer Security（TLS、TCPポート5061）を使用できます。

Cisco IOSのSIPインスペクション機能には脆弱性が存在します。リモートの攻撃者が該当デバイスのリロードを引き起こしたり、メモリリークを引き起こしたりして、システムが不安定になる可能性があります。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と引き起こされます。トランジットSIPトラフィックは、不正利用の手段となります。

この脆弱性は、Cisco Bug ID CSCti46171(登録ユーザ専用)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検査の詳細については、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。

メモリリーク検出
検出されたメモリリークは、次の例に示すように、特権EXECモードで show memory debug leaks chunksコマンドを使用して表示できます。
Router# show memory debug leaks chunks GDのブロックを追加しています…I/O Memory Address Size Alloc_pc PID Alloc-Proc Nameチャンク要素：
AllocPCアドレスサイズ親名プロセッサメモリアドレスサイズAlloc_pc PID Alloc-Proc名
4733113C 188 419CB164 129 IP入力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：メモリ不足が確認された場合にルータでメモリリークを診断する場合にのみ、お客様のネットワークですべての show memory debugコマンドを使用する必要があります。これらのコマンドは、CPUの使用率を高め、時間の影響を受けやすいプロトコルのフラップを引き起こす可能性があります。これらのコマンドは、メンテナンスウィンドウでの使用が推奨されます。

回避策

このアドバイザリに記載されている脆弱性を軽減する回避策はありません。

修正済みソフトウェア

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

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

Cisco IOS ソフトウェア

次のCisco IOSソフトウェアテーブルの各行は、Cisco IOSソフトウェアトレインに対応しています。特定のトレインに脆弱性が存在する場合、修正を含む最も古いリリースが「最初の修正済みリリース」列に表示されます。2012年3月のFirst Fixed Release for All Advisories Bundled Publication列には、Cisco IOSソフトウェアセキュリティアドバイザリバンドル公開で公開されたすべての脆弱性を修正する最初のリリースが記載されています。シスコでは、可能な限り最新のリリースにアップグレードすることを推奨しています。

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

メジャーリリース	修正済みリリースの入手可能性	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
該当する 12.0 ベースのリリースはありません。		
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
影響を受ける 12.2 ベースのリリースはありません。		
Affected 12.3-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
該当する 12.3 ベースのリリースはありません。		
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
12.4	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M

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

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

12.4JZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4JA
12.4MD	12.4(22)MD3（2012年3月30日に入手可能）	12.4(22)MD3（2012年3月30日に入手可能）
12.4MDA	12.4(24)MDA11	12.4(24)MDA11
12.4MDB	12.4(24)MDB5a	12.4(24)MDB5a
12.4MDC	脆弱性なし	脆弱性なし
12.4MR	12.4(19)MR3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。
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15.0M	脆弱性あり。最初の修正はリリース15.0M
12.4SW	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4T	12.4(24)T7 12.4(15)T17までのリリースには脆弱性はありません。	12.4(15)T17 12.4(24)T7
12.4XA	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XB	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XC	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XD	脆弱性なし	脆弱性あり。最初の修

		正はリリース15.0M
12.4XE	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XF	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XG	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XJ	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XK	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XL	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。
12.4XM	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XN	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。
12.4XP	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。
12.4XQ	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XR	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T

	12.4(15)XR10までのリリースには脆弱性はありません。	
12.4XT	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XV	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。
12.4XW	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XY	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.4XZ	脆弱性あり。最初の修正はリリース15.0M	脆弱性あり。最初の修正はリリース15.0M
12.4YA	脆弱性あり。最初の修正はリリース15.0M	脆弱性あり。最初の修正はリリース15.0M
12.4YB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4YD	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4YE	12.4(24)YE3d	12.4(24)YE3d
12.4YG	12.4(24)YG4	12.4(24)YG4
影響を受ける 15.0	First Fixed Release (修正された	2012年3月のCisco IOSソフトウェアセキ

ベースのリリース	最初のリリース)	ユリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
15.0M	15.0(1)M8	15.0(1)M8
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	脆弱性なし	15.0(1)S5 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.0SA	脆弱性なし	脆弱性なし
15.0SE	脆弱性なし	15.0(1)SE1
15.0SG	脆弱性なし	15.0(2)SG2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.0SY	脆弱性なし	15.0(1)SY1
15.0XA	脆弱性あり。最初の修正はリリース15.1T	脆弱性あり。最初の修正はリリース15.1T
15.0XO	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SG Cisco IOS XEデバイ

		スです。「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）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
15.1EY	脆弱性なし	15.1(2)EY2
15.1GC	15.1(2)GC2	15.1(2)GC2
1,510万	15.1(4)M3	15.1(4)M4（2012年3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	脆弱性なし	15.1(3)S2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.1SG	脆弱性なし	脆弱性なし
15.1SNG	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。
15.1SNH	脆弱性なし	脆弱性なし
15.1T	15.1(3)T3	15.1(3)T3
15.1XB	脆弱性あり。最初の修	脆弱性あり。最初の修

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

* Cisco Catalyst 3550シリーズスイッチは、インターネットキーエクスチェンジ(IKE)機能をサポートしており、デバイスでレイヤ3イメージを実行している場合はCisco Bug ID CSCts38429に対して脆弱です。ただし、この製品はソフトウェアメンテナンスが終了しています。 レイヤ2イメージを実行しているCisco 3550シリーズSMIスイッチはIKEをサポートしていないため、脆弱ではありません。 12.2SEベースのソフトウェアを実行する他のシスコデバイスには、この脆弱性は存在しません。

Cisco IOS XE ソフトウェア

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

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

Cisco IOS XR ソフトウェア

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

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト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。

URL

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

改訂履歴

リビジョン 1.0	2012年3月28日	初版リリース

利用規約

本アドバイザリ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。