Cisco IOS Software Zone-Based Firewall and Content Filtering Vulnerability

Advisory ID: cisco-sa-20130925-cce

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-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 1.0

For Public Release 2013 September 25 16:00 UTC (GMT)

目次

要約
該当製品
詳細
脆弱性スコア詳細
影響
ソフトウェア バージョンおよび修正
回避策
修正済みソフトウェアの入手
不正利用事例と公式発表
この通知のステータス：FINAL
情報配信
更新履歴
シスコ セキュリティ手順

要約

Cisco IOS ソフトウェアのゾーン ベース ファイアウォール（ZBFW）コンポーネントに存在する脆弱性により、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がハングまたはリロードさせられる可能性があります。

この脆弱性は、デバイスに Cisco IOS コンテンツ フィルタリングまたは HTTP 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に、特定の HTTP パケットが不適切に処理されることに起因しています。攻撃者は特定の HTTP パケットを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。この脆弱性を不正利用することにより、攻撃者は該当デバイスをハングさせたりリロードさせることができる場合があります。

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。

これらの脆弱性に対しては回避策がありません。

このアドバイザリは、次のリンクで確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-cce

注：2013 年 9 月 25 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、8 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 9 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_sep13.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 ZBFW に、HTTP ALG インスペクションまたは Cisco IOS コンテンツ フィルタリングが設定されている場合、このデバイスは脆弱性の影響を受けます。

デバイスの ZBFW に HTTP 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 running-config** コマンドを使用してください。ゾーンに関連付けられたサービス ポリシーに **service-policy http** *name* コマンドを含むポリシー マップが含まれる場合、そのデバイスには HTTP ALG が設定されています。Cisco IOS ソフトウェアが稼働し、ZBFW に HTTP ALG インスペクションが設定されているデバイスで **show running-config** コマンドを実行すると、次のような出力結果が得られます。

```
ios-fw#show running-config

< output removed for brevity >

policy-map type inspect in->out
 class type inspect filtered-hosts
  inspect
  service-policy http http_bad
 class class-default
  drop
!
zone security inside
zone security outside
zone-pair security in-to-out source inside destination outside
 service-policy type inspect in->out
< output removed for brevity > ios-fw#
```

デバイスの ZBFW に Cisco IOS コンテンツ フィルタリングが設定されているかどうかを確認するには、特権 EXEC コマンド **show policy-map type inspect zone-pair urlfilter | include URL Filtering** を使用して、出力結果を確認します。空白行は、その機能が有効になっていないことを示します。出力結果の「**URL Filtering is in**」の部分を見れば、デバイスの ZBFW に Cisco IOS コンテンツ フィルタリングが設定されていることがわかります。Cisco IOS ソフトウェアが稼働し、ZBFW の設定で Cisco IOS コンテンツ フィルタリングが有効になっているデバイスに、**show policy-map type inspect zone-pair urlfilter | include URL Filtering** コマンドを実行すると、次のような出力結果が得られます。

```
< output removed for brevity > ios-fw#
```

注： ip inspect と ip urlfilter コマンドを使用する Cisco IOS コンテンツ フィルタリングは影響を受けません。

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

Cisco IOS ソフトウェアのゾーン ベース ファイアウォール（ZFW）コンポーネントに存在する脆弱性により、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がハングまたはリロードさせられる可能性があります。

この脆弱性は、デバイスにコンテンツ フィルタリングまたは HTTP アプリケーション レイヤ ゲートウェイ インスペクションが設定されている場合に、 特定の HTTP パケットが不適切に処理されることに起因しています。攻撃者は特定の HTTP パケットを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。この脆弱性を不正利用することにより、攻撃者は該当デバイスをハングさせたりリロードさせることができる場合があります。
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 HTTP トラフィックはこの脆弱性を引き起こしません。

脆弱性のある設定条件を満たすデバイスでは、有効な HTTP パケットによって脆弱性が引き起こされる可能性があります。この脆弱性の不正利用は、IPv4 トラフィックによってのみ可能です。IPv6 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 CSCtx56174（ 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-2013-5476 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/

CSCtx56174: Cisco IOS Software Zone-Based Firewall and Content Filtering Vulnerability 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

この脆弱性が不正利用されると、該当するデバイスがクラッシュまたはハングする可能性があります。デバイスがハングした場合、回復するには電源を入れなおす必要があります。 **scheduler isr-watchdog** をサポートし、これが設定されているデバイスでは、この脆弱性が不正利用されるとリセットされ再起動します。

scheduler isr-watchdog コマンドの詳細については、「Cisco IOS Configuration Fundamentals Command Reference」（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_r1.html#wp1079401）を参照してください。

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 September 2013 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。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 September 2013 Cisco IOS Software Security 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 September 2013 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 September 2013 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 September 2013 Cisco IOS Software Security Advisory Bundled Publication
There are no affected 12.4 based releases		
Affected 15.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication
There are no affected 15.0 based releases		

Affected 15.1-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication
15.1EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
15.1GC	Vulnerable; First fixed in Release 15.1M Releases up to and including 15.1(2)GC2 are not vulnerable.	Vulnerable; First fixed in Release 15.1M
15.1M	Releases including and prior to 15.1(4)M1 are not vulnerable.First fixed in 15.1(4)M6.	15.1(4)M7
15.1MR	Not vulnerable	Vulnerable; contact your support organization the instructions in Obtaining Fixed Software se of this advisory.
15.1MRA	Not vulnerable	15.1(3)MRA2
15.1S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S6 Cisco IOS XE devices: Please see Cisco IOS X Software Availability
15.1SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(2)SG1 Cisco IOS XE devices: Please see Cisco IOS X Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization the instructions in Obtaining Fixed Software se of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization the instructions in Obtaining Fixed Software se of this advisory.
15.1SNI	Not vulnerable	Vulnerable; contact your support organization the instructions in Obtaining Fixed Software se of this advisory.
15.1SVD	Not vulnerable	Not vulnerable
15.1SVE	Not vulnerable	Not vulnerable
15.1SVF	Not vulnerable	Not vulnerable
15.1SY	Not vulnerable	15.1(1)SY2; Available on 28-OCT-13 15.1(2)SY
15.1T	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.1XO	Not vulnerable	Not vulnerable
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication**
15.2E	Not vulnerable	Not vulnerable
15.2GC	15.2(4)GC	Vulnerable; migrate to any release in 15.4T
15.2JA	Not vulnerable	15.2(4)JA1
15.2JAX	Not vulnerable	Vulnerable; contact your support organization the instructions in Obtaining Fixed Software se of this advisory.
15.2JB	Not vulnerable	15.2(2)JB2
15.2JN	Not vulnerable	Not vulnerable
15.2M	Not vulnerable	15.2(4)M4
15.2S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(4)S4 Cisco IOS XE devices: Please see Cisco IOS X Software Availability
15.2SA	Not vulnerable	15.2(2)SA
15.2SNG	Not vulnerable	Vulnerable; contact your support organization the instructions in Obtaining Fixed Software se

		of this advisory.
15.2SNH	Not vulnerable	Vulnerable; contact your support organization the instructions in Obtaining Fixed Software se of this advisory.
15.2SNI	Not vulnerable	Vulnerable; First fixed in Release 15.3S
15.2T	15.2(1)T4 15.2(3)T4	15.2(3)T4
Affected 15.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication**
There are no affected 15.3 based releases		

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、2013 年 9 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

これらの脆弱性に対しては回避策がありません。

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を入手することができます。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。

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（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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、お客様のサービス リクエストの処理中に発見されました。

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-20130925-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 1.0	2013-September-25	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。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。