Cisco IOS Software Malformed Border Gateway Protocol Attribute Vulnerability

Advisory ID: cisco-sa-20120926-bgp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

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 Update 2012 October 4 15:33 UTC (GMT)

For Public Release 2012 September 26 16:00 UTC (GMT)

内容

要約

Cisco IOS ソフトウェアの Border Gateway Protocol（BGP）ルーティング プロトコル機能には、脆弱性が存在します。

この脆弱性は、ルータが既存の BGP セッションのピアから不正なアトリビュートを受信した場合に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に成功した場合、すべての BGP セッションがリセットされる可能性があります。この脆弱性が繰り返し悪用されると、再収束中にパケットを BGP ネイバーにルーティングできなくなる可能性があります。

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。この脆弱性に対する回避策はありません。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-20120926-bgp

注：2012 年 9 月 26 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。8 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 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解決する Cisco IOS ソフトウェア リリース、および 2012 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_sep12.html

該当製品

この脆弱性は、Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および Cisco IOS XE ソフトウェアに影響を及ぼします。

脆弱性が存在する製品

該当する Cisco IOS ソフトウェア バージョンを使用している Cisco IOS ルータで BGP ルーティングが有効になっており、少なくとも 1 つの BGP ネイバー セッションが確立している場合に、脆弱性が存在する可能性があります。該当バージョンの詳細については、下記の「ソフトウェア バージョンおよび修正」を参照してください。

Cisco IOS XR を実行するデバイスが次の **両方**の条件を満たす場合、デバイスは脆弱性のある設定となっています。

1. BGP mVPN ルーティングが有効で、ネイバーが設定されている場合。コマンドの設定例を次に示します。

    router bgp <as-id>
    address-family <ipv4 | ipv6> mvpn
    neighbor <neighbor-ip>

2. ネイバー セッションが確立している場合。

Note: Cisco IOS XRに おいて、上記に記載されているように *address-family <ipv4|ipv6> mvpn* の設定のみが脆弱性を持っています。 MDT (マルチキャスト分散ツリー) を伴う BGP mVPN は影響をうけません。

Cisco IOS を実行するデバイスが次の **両方**の条件を満たす場合、デバイスは脆弱性のある設定となっています。

1. BGP ルーティングが有効で、ネイバーが設定されている場合。設定されているコマンドの例を次に示します。

    router bgp <as-id>

    neighbor <neighbor-ip>

2. BGP ネイバー セッションが確立している場合。

BGP セッションが確立されているかどうかは、Cisco IOS ソフトウェアの **show ip bgp summary** コマンドで確認できます。Cisco IOS XR ソフトウェアでは、 **show bgp <ipv4 | ipv6> mvpn all summary** コマンドで BGP セッションが確立されているかどうかを確認できます。次の例は、2 つのネイバー セッションが確立している IOS ルータの出力結果です。

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 **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

脆弱性が存在しない製品

Cisco IOS ルータは、BGP が実行されていない場合、または BGP でネイバー セッションが確立されていない場合、脆弱性は存在しません。他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。Cisco NX-OS ソフトウェアは影響を受けません。

次の例は、BGP が有効で、ネイバーが 2 つ設定されており、リモートの BGP ピアとはセッションを確立していないルータの出力結果です。

詳細

Cisco IOS ソフトウェアの BGP ルーティング プロトコル機能には、脆弱性が存在します。この脆弱性は、Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および Cisco IOS XE ソフトウェアに影響を及ぼします。Cisco NX-OS ソフトウェアは影響を受けません。

この脆弱性は、ルータが既存の BGP セッションのピアから不正なアトリビュートを受信した場合に引き起こされる可能性があります。少なくとも 1 つの BGP ネイバー セッションが確立されている場合に、脆弱性の影響を受けます。

この脆弱性の不正利用に成功した場合、すべての BGP ピアがリセットされる可能性があります。この脆弱性が繰り返し悪用されると、再収束中にパケットを BGP ネイバーにルーティングできなくなる可能性があります。

この脆弱性は、Cisco Bug ID CSCtt35379（ 登録ユーザのみ ）および CSCty58300（ 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-2012-4617 が割り当てられています。対応する Cisco IOS XR Bug ID は、 CSCtz63248（ 登録ユーザのみ ）と CSCtz62914（ 登録ユーザのみ ）です。

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/

CSCtt35379 - BGP Processing Enhancements and CSCty58300 - BGP Processing Enhancements Calculate the environmental score of					
CVSS Base Score - **7.1**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - **5.9**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtz63248 - Improper checks for BGP attributes and CSCtz62914 - BGP handling of invalid attribute needs to be more robust Calculate the environmental score of

CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、すべての BGP ピアがリセットされる可能性があります。この脆弱性が繰り返し悪用されると、再収束中にパケットを BGP ネイバーにルーティングできなくな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 アーカイブや、本アドバイザリ以降に公開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 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されているすべての脆弱性の修正を含む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 Septe 2012 Cisco IOS Software Security Advisory Bund 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 Septe 2012 Cisco IOS Software Security Advisory Bund 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 Septe 2012 Cisco IOS Software Security Advisory Bunc 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 Septe 2012 Cisco IOS Software Security Advisory Bunc 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 Septe 2012 Cisco IOS Software Security Advisory Bunc 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 Septe 2012 Cisco IOS Software Security Advisory Bunc Publication**
There are no affected 15.1 based releases		
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the Septe 2012 Cisco IOS Software Security Advisory Bunc Publication**
15.2GC	Not vulnerable	Releases prior to 15.2(3)GC are vulnerable; Rele 15.2(3)GC and later are not vulnerable.First fixed Release 15.2T
15.2JA	Not vulnerable	Not Vulnerable
15.2M	Not vulnerable	Not vulnerable
15.2S	15.2(1)S0a 15.2(1)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(1)S2 15.2(2)S1 15.2(4)S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.2SNG	Not vulnerable	Not vulnerable
15.2T	Not vulnerable	15.2(1)T3 15.2(2)T2 15.2(3)T2; Available on 12-OCT-12

Cisco IOS XE ソフトウェア

Cisco IOS XE は、このアドバイザリに記載されている脆弱性の影響を受けます。

Cisco IOS XE Software Release	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication
2.1.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.2.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.3.x	Not	Vulnerable; migrate to 3.6.0S or later.

	vulnerable	
2.4.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.5.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.6.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.1.xS	Not vulnerable	3.1.4S
3.1.xSG	Not vulnerable	Vulnerable; migrate to 3.2.5SG or later.
3.2.xS	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.2.xSG	Not vulnerable	3.2.5SG
3.2.xSO	Not vulnerable	Vulnerable; migrate to 3.3.1SG or later.
3.3.xS	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.3xSG	Not vulnerable	3.3.1SG
3.4.xS	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.5.xS	3.5.2S	Vulnerable; migrate to 3.6.0S or later.
3.6.xS	Not vulnerable	Not vulnerable
3.7xS	Not vulnerable	Not vulnerable

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェア リリース 4.1.0、4.1.1、4.1.2、4.2.0、4.2.1、および 4.2.2 は、このアドバイザリに記載されている脆弱性の影響を受けます。

Release	Platform	CSCtz62914 SMU ID	CSCtz63248 SMU ID
4.1.0	c12k	AA06458	AA06464
4.1.0	CRS	AA06437	AA06399
4.1.0	asr9k	AA06449	AA06444
4.1.1	c12k	AA06459	AA06465
4.1.1	CRS	AA06438	AA06400
4.1.1	asr9k	AA06450	AA06445
4.1.2	c12k	AA06460	AA06466
4.1.2	CRS	AA06439	AA06401
4.1.2	asr9k	AA06451	AA06446
4.2.0	c12k	AA06461	AA06467
4.2.0	CRS	AA06440	AA06402
4.2.0	asr9k	AA06452	AA06447
4.2.0	asr9k (PX)	AA06453	AA06448
4.2.1	c12k	AA06462	AA06546
4.2.1	CRS	AA06441	AA06547
4.2.1	asr9k	AA06454	AA06548
4.2.1	asr9k (PX)	AA06455	AA06549
4.2.2	asr9k	AA06581	AA06550
4.2.2	asr9k (PX)	AA06582	AA06551

回避策

この脆弱性に対する回避策はありません。

有用な参考資料として、ホワイト ペーパーの『Protecting BGP』があります。
http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html

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。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、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。

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-20120926-bgp

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 1.1	2012-October-04	Added mVPN MDT note in the "Vulnerable Products" section.
Revision 1.0	2012-September-26	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。