Cisco IOS BGP属性破損の脆弱性

アドバイザリーID : cisco-sa-20010510-ios-bgp-attr
初公開日 : 2001-05-10 15:00
バージョン 1.1 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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

ボーダーゲートウェイプロトコル(BGP)UPDATEには、ネットワーク層到達可能性情報(NLRI)と、宛先へのパスを記述する属性が含まれています。Cisco IOSルータでは、認識されていない推移属性が受信された場合のクラッシュから、認識されていない推移属性をクリアしようとする後の障害に至るまで、障害が発生する可能性があります。特定の設定が影響を受けますが、一般的な設定については後述します。この障害は、他のベンダーのBGP実装の誤動作が原因で発見されました。回避策はありません。該当するお客様には、修正済みコードへのアップグレードが推奨されます。

この脆弱性には、Cisco Bug ID CSCdt79947が割り当てられています。

このアドバイザリの全文は、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010510-ios-bgp-attrに掲載されています。

該当製品

脆弱性のある製品

着信ルートマップを使用したBGP4プレフィクスフィルタリングを含む設定には脆弱性が存在します。プレフィクス着信ルートマップフィルタリングを使用したBGPはCisco IOS®ソフトウェアバージョン11.2で導入されました。次の表に示すCisco IOSソフトウェアのバージョン11.CCとその派生物、11.2とその派生物、11.3、11.3T、12.0、12.0S、および12.0から抜粋した特殊なブランチがすべて影響を受けます。12.1、12.0(5)T、12.2、12.0ST、および12.1(E)に基づくCisco IOSソフトウェアのバージョンは、この脆弱性の影響を受けません。次の製品は、この不具合のCisco IOSソフトウェアリリースが稼働している場合に影響を受けます。シスコ製品で該当するIOSが稼働し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 versionコマンドを発行します。Cisco IOSソフトウェアは、「Internetwork Operating System

Software」または「IOS(tm)」ソフトウェアとして識別され、バージョン番号が表示されます。他のシスコデバイスには、show versionコマンドがないか、異なる出力が返されます。ルータから取得したバージョン番号を、次の「ソフトウェアバージョンと修正」セクションに示すバージョンと比較します。

該当するCisco IOSソフトウェアリリースが稼働しているシスコデバイスには、次のものがあります。

- AGS/MGS/CGS/AGS+、IGS、RSM、800、ubr900、1000、1400、1500、1600、1700、2500、2600、3000、3600、3800、4000、4500、470にあるCiscoルータ 0、AS5200、AS5300、AS5800、6400、7000、7200、ubr7200、7500、および12000シリーズ。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアを実行しているが、BGPをサポートしていないため脆弱ではないシスコデバイスには、次のものがあります。

- LS1010 ATMスイッチの最新バージョン。
- Catalyst 2900XL LANスイッチは、IOSを実行している場合にのみ使用できます。
- Catalyst 1900、2800、2900、3000、および5000シリーズLANスイッチ。
- Cisco DistributedDirectorです。

Cisco IOSソフトウェアを実行していない場合、この脆弱性の影響を受けません。BGPを実行していない場合、この脆弱性の影響を受けません。

Cisco IOSソフトウェアが稼働しておらず、この不具合の影響を受けないシスコ製品には次のものが含まれますが、これらに限定されません。

- 700シリーズのダイヤルアップルータ（750、760、および770シリーズ）は影響を受けません。
- Catalyst 6000は、IOSを実行していない場合は該当しません。
- IGXおよびBPXラインのWANスイッチング製品は影響を受けません。
- MGX（以前のAXISシェルフ）は影響を受けません。
- ホストベースのソフトウェアは影響を受けません。
- Cisco PIX Firewallは該当しません。
- Cisco LocalDirectorは該当しません。
- Cisco Cache Engineは該当しません。

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

ボーダーゲートウェイプロトコル(BGP)UPDATEには、ネットワーク層到達可能性情報(NLRI)と

、宛先へのパスを記述する属性が含まれています。各パス属性は、タイプ、長さ、値(TLV)オブジェクトです。この障害は、メモリ不良の結果として発生し、特定の着信ルートフィルタリングを使用する設定でのみ発生します。この障害は、他のベンダーのBGP実装の誤動作が原因で発見されました。回避策はありません。

回避策

この脆弱性に対する既知の回避策はありません。修正済みバージョンにアップグレードしてください。

修正済みソフトウェア

次の表に、影響を受けることが確認されているCisco IOSソフトウェアリリースと、推奨される修正済みバージョンの入手が可能になる最も早い予定日をまとめます。日付は常に暫定的なものであり、変更される可能性があります。

表の各行に、リリース群、および対象のプラットフォームまたは製品を示します。特定のリリーストレインに脆弱性が存在する場合、修正を含む最初のリリースと、各リリースの提供予定日が「Rebuild」、「Interim」、および「Maintenance」の各列に表示されます。特定の列のリリースより前（最初の修正リリースより前）のトレインのリリースを実行しているデバイスは脆弱であることが確認されており、少なくとも示されたリリースまたは以降のバージョン（最初の修正リリースのラベルより後）にアップグレードする必要があります。

リリースを選択するときは、次の定義を念頭においてください。

- メンテナンス
  表の特定の行にあるラベルの、最も頻繁にテストされ、推奨されるリリース。
- リビルド
  同じトレインの以前のメンテナンスリリースまたはメジャーリリースから構築され、特定の不具合に対する修正が含まれています。テストの回数は少なくなりますが、修復に必要な最小限の変更のみが含まれています。
- Interim
  メンテナンスリリース間に定期的に構築され、テストの頻度が少ない。暫定イメージは、脆弱性に対処する適切なリリースが他にない場合にのみ選択し、可能な限り早急に次のメンテナンスリリースにアップグレードする必要があります。暫定リリースは製造部門を通じて入手することはできず、通常はCisco TACと事前に調整を行わないと、CCOからダウンロードできません。

次の表では、特定のソフトウェアリリースに対してリビルドまたはメンテナンスが計画されていない場合に、論理的な置き換えソフトウェアが推奨されています。お客様は、計画されたアップグレードが要件を満たしていることを確認する必要があります。詳細については、各Cisco IOSトレインのIOSリリースノートを参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/software/index.htmいずれの場合も、アップグレ

ードする機器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。情報が明確でない場合は、この通知の後半で説明するように、Cisco TACに連絡して支援を求めてください。

Cisco IOSソフトウェアのリリース名と省略形の詳細については、http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.htmlを参照してください。

<table>
<tr><th>リリース群</th><th>イメージまたはプラットフォームの説明</th><th colspan="3">修正リリースのアベイラビリティ</th></tr>
<tr><td colspan="2">11.0 ベースのリリース</td><td>リビルド</td><td>Interim</td><td>メンテナンス</td></tr>
<tr><td>11.0</td><td>すべてのプラットフォーム用のメジャーGDリリース</td><td colspan="3">脆弱性なし</td></tr>
<tr><td colspan="2">11.1 ベースのリリース</td><td>リビルド</td><td>Interim</td><td>メンテナンス</td></tr>
<tr><td>11.1</td><td>すべてのプラットフォームのメジャーリリース</td><td colspan="3">脆弱性なし</td></tr>
<tr><td>11.1AA</td><td>アクセスサーバ用EDリリース：1600、3200、および5200シリーズ。</td><td colspan="3">脆弱性なし</td></tr>
<tr><td rowspan="2">11.1CA</td><td rowspan="2">7500、7200、7000、およびRSPのプラットフォーム固有のサポート</td><td colspan="3">エンジニアリング終了</td></tr>
<tr><td colspan="3">スケジュールなし</td></tr>
<tr><td>11.1CC</td><td>ISPトレイン：7500、7200、7000、およびRSPでのFIB、CEF、お</td><td colspan="3">11.1(36)CC2</td></tr>
</table>

	およびNetFlowのサポートを追加	2001年5月29日		
11.1CT	7500、7200、7000、およびRSPでのタグスイッチングのサポートを追加	エンジニアリング終了		
		12.0STへのアップグレードを推奨		
11.1IA	Distributed Directorのみ	脆弱性なし		
11.2 ベースのリリース		リビルド	Interim	メンテナンス
11.2	メジャーリリース、一般導入	エンジニアリング終了		
		スケジュールなし		
11.2BC	7500、7000、およびRSPでのIBMネットワーキング、CIP、およびTN3270のプラットフォーム固有のサポート	エンジニアリング終了		
		12.1(8)へのアップグレードを推奨		
11.2F	すべてのプラットフォームの機能トレイン	エンジニアリング終了		
		アップグレードを推奨		
11.2GS	12000 GSRをサポートする早期導入リリース	エンジニアリング終了		
		12.0(17)Sへのアップグレードを推奨		
11.2P	新しいプラットフォームのサポート	エンジニアリング終了		

		12.0(17)へのアップグレードを推奨		
11.2SA	Catalyst 2900XLスイッチのみ	脆弱性なし		
11.2WA3	LightStream 1010ATMスイッチ	脆弱性なし		
11.2(4)XA	1600および3600の初期リリース	エンジニアリング終了		
		アップグレードを推奨		
11.2(9)XA	5300の初期リリースと3600のデジタルモデムサポート	エンジニアリング終了		
		アップグレードを推奨		
11.3 ベースのリリース		リビルド	Interim	メンテナンス
11.3	すべてのプラットフォームのメジャーリリース	エンジニアリング終了		
		12.0(17)へのアップグレードを推奨		
11.3AA	ダイヤルプラットフォームおよびアクセスサーバ用ED:5800、5200、5300、7200	エンジニアリング終了		
		12.0(17)へのアップグレードを推奨		
11.3DA	ISP DSLAM 6200プラットフォームの初期導入トレイン	エンジニアリング終了		
		12.1DAへのアップグレードを推奨		

11.3 DB	6400用のISP/Telco/PTT xDSLブロードバンドコンセントレータプラットフォーム(NRP)の初期配備トレイン	エンジニアリング終了
		12.1DBへのアップグレードを推奨
11.3HA	ISR 3300用の短期EDリリース（SONET/SDHルータ）	エンジニアリング終了
		12.0へのアップグレードを推奨
11.3 MA	MC3810機能のみ	使用不可
		スケジュールなし
11.3NA	Voice over IP、メディアコンバージェンス、各種プラットフォーム	エンジニアリング終了
		12.1へのアップグレードを推奨
11.3T	早期導入者向けの豊富な機能を備えた早期導入メジャーリリース	エンジニアリング終了
		12.0(17)へのアップグレードを推奨
11.3WA4	Catalyst 5000 RSM、4500、4700、7200、7500、LightStream 1010用のMultilayer Switching（MLS；マルチレイヤスイッチング）およびMultiprotocol over ATM機能	エンジニアリング終了
		アップグレードを推奨
11.3(2)XA	ubr7246および2600の概要	エンジニアリング終了

<table>
<tr><td></td><td></td><td colspan="3">アップグレードを推奨</td></tr>
<tr><td colspan="2">12.0 ベースのリリース</td><td>リビルド</td><td>Interim</td><td>メンテナンス</td></tr>
<tr><td>12.0</td><td>すべてのプラットフォーム向けの一般導入リリース</td><td></td><td></td><td>12.0(17) 2001-Apr-23</td></tr>
<tr><td rowspan="2">12.0DA</td><td rowspan="2">xDSLサポート：6100、6200</td><td colspan="3">使用不可</td></tr>
<tr><td colspan="3">12.1DAへのアップグレードを推奨</td></tr>
<tr><td rowspan="2">12.0DB</td><td rowspan="2">ノードスイッチプロセッサ(NSP)のCisco 6400 Universal Access Concentrator(UAC)をサポートするEarly Deployment(ED)リリース</td><td colspan="3">使用不可</td></tr>
<tr><td colspan="3">12.1DBへのアップグレードを推奨</td></tr>
<tr><td rowspan="2">12.0DC</td><td rowspan="2">Early Deployment(ED)リリース：Node Route Processor(NRP)用のCisco 6400 Universal Access Concentrator(UAC)をサポートします。</td><td colspan="3">使用不可</td></tr>
<tr><td colspan="3">12.1DCへのアップグレードを推奨</td></tr>
<tr><td rowspan="2">12.0S</td><td rowspan="2">コア/ISPサポート：GSR、RSP、c7200</td><td>12.0(15)S3、12.0(16)S1</td><td>12.0(16.06)S</td><td>12.0(17)S</td></tr>
<tr><td>2001年4月23日
2001年4月30日</td><td></td><td>2001年5月7日</td></tr>
</table>

12.0SC	ケーブル/ブロードバンドISP:ubr7200	脆弱性なし		
12.0SL	10000 ESR:c10k	脆弱性なし		
12.0ST	Cisco IOSソフトウェアリリース12.0STは、サービスプロバイダー(ISP)向けのCisco 7200、7500/7000RSP、および12000(GSR)シリーズルータ用のEarly Deployment（ED；初期配備）リリースです。	脆弱性なし		
12.0T	Early Deployment(ED):VPN、Distributed Director、各種プラットフォーム			12.0(5)T
12.0W5	Catalystスイッチ：cat2948g-l3、cat4232	12.0(10)W5(18g) 2001-Apr-20		
	cat8510c、cat8540c、c6msm、ls1010、cat8510m、cat8540m、c5atm			12.0(16)W5(21) 2001年5月21日
12.0WT	Catalystスイッチ：cat4840g	脆弱性なし		
12.0XA	Early Deployment(ED)：プラ	使用不可		

	ットフォームが限られている	12.1へのアップグレードを推奨
12.0XB	短期初期配備リリース	使用不可
		12.1へのアップグレードを推奨
12.0XC	Early Deployment(ED)：プラットフォームが限られている	使用不可
		12.1へのアップグレードを推奨
12.0XD	Early Deployment(ED)：プラットフォームが限られている	使用不可
		12.1へのアップグレードを推奨
12.0XE	Early Deployment(ED)：プラットフォームが限られている	脆弱性なし
12.0XF	Early Deployment(ED)：プラットフォームが限られている	使用不可
		12.1へのアップグレードを推奨
12.0XG	Early Deployment(ED)：プラットフォームが限られている	使用不可
		12.1へのアップグレードを推奨
12.0XH	Early Deployment(ED)：プラットフォームが限られ	使用不可

	ている	12.1へのアップグレードを推奨
12.0XI	Early Deployment(ED)：プラットフォームが限られている	使用不可
		12.1へのアップグレードを推奨
12.0XJ	Early Deployment(ED)：プラットフォームが限られている	使用不可
		12.1へのアップグレードを推奨
12.0XK	Early Deployment(ED)：プラットフォームが限られている	脆弱性なし
12.0XL	Early Deployment(ED)：プラットフォームが限られている	脆弱性なし
12.0XM	短期初期配備リリース	脆弱性なし
12.0XN	Early Deployment(ED)：プラットフォームが限られている	脆弱性なし
12.0XP	Early Deployment(ED)：プラットフォームが限られている	脆弱性なし
12.0XQ	短期初期配備リリース	脆弱性なし

12.0XR	短期初期配備リリース	脆弱性なし		
12.0XS	短期初期配備リリース	脆弱性なし		
12.0XU	Early Deployment(ED)：プラットフォームが限られている	脆弱性なし		
12.0XV	短期初期配備リリース	脆弱性なし		
12.1ベース以降のリリース		リビルド	Interim	メンテナンス
12.1	すべてのプラットフォーム向けの一般導入リリース	脆弱性なし		
注意事項				
*すべての日付は概算であり、変更される可能性があります。 通常のメンテナンス リリースと比較した場合、暫定リリースに対しては厳格なテストが実施されていないため、重大なバグが含まれている可能性があります。				

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

シスコには、この脆弱性の悪意のあるエクスプロイトに関する報告はありません。この障害は、他のベンダーのBGP実装の誤動作が原因で発見され、これが原因で一連のクラッシュが発生し、この問題が特定されました。

シスコでは、この通知の日付より前には、この脆弱性に関する公式発表はありません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010510-ios-bgp-attr

改訂履歴

リビジョン 1.1	2001-November-29	一部のIOSバージョンに対するアップグレードの推奨事項を変更
リビジョン 1.0	2001年5月10日	初版リリース

利用規約

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。