Cisco IOSの不正なBGPパケットによるリロード

アドバイザリーID : cisco-sa-20050126-bgp CVE-2005-0196
初公開日 : 2005-01-26 16:00
バージョン 1.5 : 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

IOS Border Gateway Protocol(BGP)を実行しているシスコデバイスは、不正なBGPパケットによるサービス拒否(DoS)攻撃に対して脆弱です。bgp log-neighbor-changesコマンドまたはsnmp-server enable traps bgpコマンドが設定されているデバイスにのみ脆弱性が存在します。BGPプロトコルはデフォルトでは有効になっていないため、明示的に定義されたピアからのトラフィックを受け入れるように設定する必要があります。悪意のあるトラフィックが設定された信頼できるピアから送信されていると思われない限り、不正なパケットを挿入することは困難です。

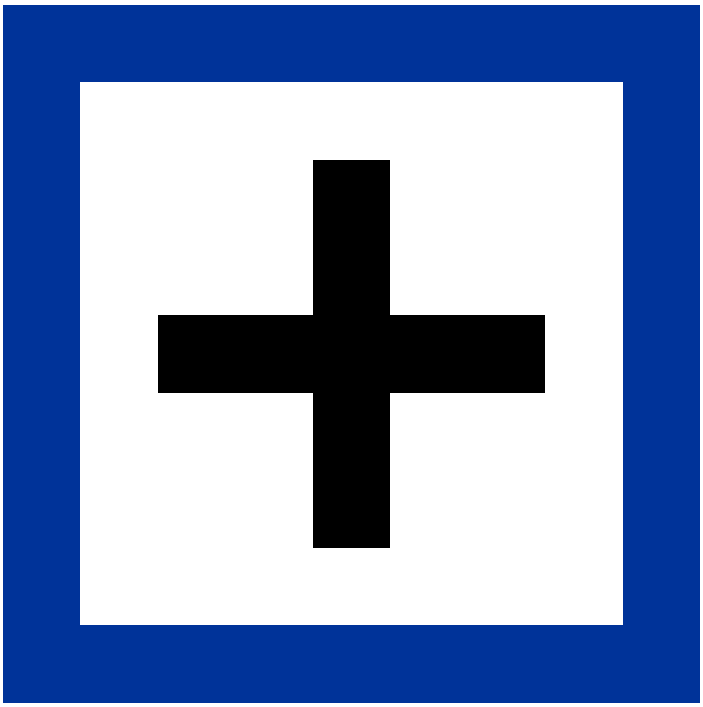
シスコでは、この問題に対処する無償のソフトウェアを提供しています。

この問題はCERT/CC VU#689326で追跡されています。

このアドバイザリは https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-bgp に掲載されています。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。



脆弱性のある製品

この脆弱性は、9.x、10.x、11.x、および12.xを含む、BGPプロトコルのサポート開始以降のCisco IOSの未修正バージョンに存在します。この問題は、BGPルーティングが設定されていて、bgp log-neighbor-changesコマンドまたはsnmp-server enable traps bgpが設定されているすべてのCiscoデバイスに影響を与えます。12.0(22)S、12.0(11)ST、12.1(10)E、12.1(10)以降のソフトウェアでは、bgp log-neighbor-changesコマンドはデフォルトでオンになっています。

Cisco IOS XRも該当します。

BGPプロセスを実行しているルータの設定には、次の行が含まれます。

```
router bgp <AS number>
```

デバイスに影響を与えるには、次の設定コマンドのいずれかまたは両方を有効にする必要があります。

<#root>

bgp log-neighbor-changes

または

<#root>

snmp-server enable traps bgp

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、show version コマンドを発行してシステム バナーを表示します。Cisco IOSソフトウェアは、「Internetwork Operating System Software」または単に「IOS ®」と表示されます。 出力の次の行では、イメージ名がカッコで囲まれて表示され、その後に「Version」とIOSリリース名が続きます。その他の Cisco 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。

次の例は、IOSリリース12.0(3)が稼働し、インストールされているイメージ名がC2500-IS-Lであるシスコ製品を示しています。

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

リリーストレインラベルは「12.0」です。

次の例は、IOSリリース12.0(2a)T1を実行し、イメージ名がC2600-JS-MZの製品を示しています。

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Cisco IOSリリースの命名の詳細については、http://www.cisco.com/warp/public/620/1.htmlを参照してください。

脆弱性を含んでいないことが確認された製品

脆弱性の影響を受けないことが確認された製品には、Cisco GuardなどのCisco IOSを実行しないデバイス、BGPに参加できない製品、またはBGPを設定できない製品が含まれます。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

Border Gateway Protocol（BGP；ボーダーゲートウェイプロトコル）は、RFC 1771で定義されているルーティングプロトコルで、大規模ネットワークでのIPルーティングを管理するために設計されています。BGPネイバーの変更がログに記録される際に、不正な形式のBGPパケットがすでにインターフェイスでキューイングされている場合、BGPプロトコルが有効なCisco IOSソフトウェアの脆弱なバージョンが稼働している該当シスコデバイスでは、リロードが発生します。bgp log-neighbor-changesまたはsnmp-server traps enable bgpが設定されていない限り、このデバイスは脆弱ではありません。

不正な形式のパケットは、悪意のある送信元から送信されるだけではありません。エラーで特定の不正なパケットを生成する別のBGPスピークルータなどの有効なピアリングデバイスがこの動作をトリガーする可能性があります。

ただし、いずれの場合も、パケットは明示的に設定されたIPアドレスから送信される必要があります。

BGPはTransport Control Protocol（TCP；トランスポート制御プロトコル）上で動作します。TCPは信頼性の高いトランスポートプロトコルであり、以降のメッセージを受け入れる前に、有効な3ウェイハンドシェイクを必要とします。Cisco IOSのBGP実装では、接続を確立する前にネイバーを明示的に定義する必要があり、トラフィックはそのネイバーから到達しているように見える必要があります。これらの実装の詳細は、不正な送信元からCisco IOSデバイスにBGPパケットを悪意をもって送信することを非常に困難にします。

この不具合は、リモートで悪用できないと見なされる他の手段によって引き起こされる可能性もあります。show ip bgp neighborsコマンドまたはdebug ip bgpコマンドを使用すると、デバイスが以前に不正なパケットを受信した場合にルータがリロードする可能性があります。

また、SNMP管理ステーションを使用してSNMPオブジェクト識別子(OID)bgpPeerEntry.bgpPeerLastError(1.3.6.1.2.1.15.3.1.14)をポーリングすると、デバイスがリセットされる場合があります。これは、デバイスが不正なパケットを受信し、BGPセッションがリセットされた後にのみ発生する可能性があります。

無効なBGPパケットを受信したCisco IOSデバイスはリセットされ、完全に機能するまでに数分

かかる場合があります。この脆弱性が繰り返し悪用されると、長時間にわたるDoS攻撃が発生する可能性があります。この問題は、Bug ID CSCee67450(登録ユーザ専用)に記述されています。

Cisco IOS XRデバイスがBGPプロセスを再起動します。すべてのセッションがドロップされ、BGPプロセスはピアとのセッションを再確立する必要があります。他のルーティングプロトコルは影響を受けません。

グレースフルリスタートが有効になっている場合は、転送に影響はありません。

IOS XRでは、BGPプロセスはデフォルトで必須ではありません。ユーザがBGPプロセスを必須に明示的に設定していない限り、IOS XRデバイスはリロードされません。

回避策

回避策の効果は、製品の組み合わせ、ネットワークトポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。該当する製品とリリースは多岐に渡るので、サービス プロバイダーやサポート機関に連絡し、ネットワーク内で使用するのに最も適した回避策を確認してから、実際に配備することを推奨いたします。

- 設定コマンドbgp log-neighbor-changesを削除します。この機能はBGPピアの状態を監視するために使用され、この機能を削除するとネットワーク監視機能が低下する可能性があります。このコマンドの詳細については、http://www.cisco.com/en/US/docs/ios/12_3/iproute/command/reference/ip2_a1g.html#wp1040601を参照してください。

ネットワークベストプラクティスの手法を使用すると、ネットワークインフラストラクチャ攻撃の可能性を大幅に低減できます。この場合のリスクを軽減できるベストプラクティスは次のとおりです。

BGP MD5

通常の状況では、シーケンス番号のチェックなど、TCPプロトコルに固有のセキュリティ要因により、この問題を不正利用するために適切なパケットを偽造することは困難ですが、可能です。Cisco IOSデバイスでBGP MD5認証を設定すると、リモートピアから有効なパケットを偽造するために必要な作業が大幅に増加します。有効なBGPピアが無効なパケットを生成した場合、ピアリングセッションは保護されません。

これは、次の例に示すように設定できます。

```
<#root>

router(config)#

router bgp
```

```
 router(config-router)#
neighbor
            password
```

両方のピアで同時に同じ共有MD5シークレットを設定する必要があります。そうしないと、既存のBGPセッションが中断され、両方のデバイスで同じシークレットが設定されるまで、新しいセッションは確立されません。BGPの設定方法の詳細については、次の文書を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a0

シークレットを設定したら、定期的に変更することをお勧めします。正確な期間は会社のセキュリティポリシーに適合している必要がありますが、数ヵ月以内である必要があります。シークレットを変更する場合も、両方のデバイスで同時に行う必要があります。そうしないと、既存のBGPセッションが中断されます。ただし、Cisco IOSソフトウェアリリースに、接続の両側で修正が組み込まれたCSCdx23494(登録ユーザ専用)が含まれている場合は例外です。この修正を適用すると、MD5シークレットが一方の側でのみ変更された場合にBGPセッションが終了しなくなります。ただし、両方のデバイスで同じシークレットが設定されるか、両方のデバイスからシークレットが削除されるまで、BGPアップデートは処理されません。

Infrastructure Access Control List（iACL; インフラストラクチャ アクセス コントロール リスト）

ネットワークを移動するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。インフラストラクチャACLはネットワークセキュリティのベストプラクティスと考えられており、ここでの特定の脆弱性に対する追加の保護を提供するだけでなく、優れたネットワークセキュリティに対する長期的な付加機能として考慮する必要があります。ホワイトペーパー『Protecting Your Core: Infrastructure Protection Access Control Lists』では、インフラストラクチャ保護ACLのガイドラインと推奨される導入方法について説明しています。

http://www.cisco.com/warp/public/707/iacl.html

IOS XRの回避策

Cisco IOS XRのユーザは、「warning」のレベルで「debug bgp」を有効にしないことや、より詳細な設定を行うことや、bgpネイバーの状態の変更をログに記録しないことによって、この脆弱性の影響を回避できます。

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/en/US/products/products_security_advisories_listing.htmlおよび後続のアドバイザリも参照して、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。情報が不明な場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

IOS XRソフトウェアを実行しているシスコのお客様は、修復されたソフトウェアについてシスコのTACにお問い合わせください。

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	リビルド	メンテナンス リリース
12.0	12.0(28b)	
12.0DA	脆弱性あり。TACに連絡	
12.0DB	12.3(4)T11以降に移行	
12.0DC	12.3(4)T11以降に移行	
12.0S	12.0(25)S5	
	12.0(26)S2d	
	12.0(26)S5	

	12.0(27)S2d	
	12.0(27)S4	
	12.0(28)S1	
		12.0(29)S
12.0SC	脆弱性あり。TACに連絡	
12.0SP	12.0S以降に移行	
12.0ST	12.0(26)S5以降に移行	
12.OSV	12.0(27)SV4	
12.0SX	脆弱性あり。TACに連絡	
12.0SY	12.0(26)S5以降に移行	
12.0SZ	12.0(26)S5以降に移行	
12.0W5		12.0(28)W5 （31）
12.0WC	脆弱性あり。TACに連絡	
12.0WT	脆弱性あり。TACに連絡	
12.0WX	脆弱性あり。TACに連絡	

12.0XA	最新の12.1への移行が必要	
12.0XB	12.0(1)T以降に移行	
12.0XC	最新の12.1への移行が必要	
12.0XD	最新の12.1への移行が必要	
12.0XE	最新の12.1Eへの移行	
12.0XF	脆弱性あり。TACに連絡	
12.0XG	最新の12.1への移行が必要	
12.0XH	12.1以降に移行	
12.0XI	12.1以降に移行	
12.0XJ	最新の12.1への移行が必要	
12.0XK	最新の12.2への移行が必要	
12.0XL	最新の12.2への移行が必要	
12.0XM	12.1以降に移行	

12.0XN	最新の12.1への移行が必要	
12.0XP	脆弱性あり。TACに連絡	
12.0XQ	12.1以降に移行	
12.0XR	最新の12.2への移行が必要	
12.0XS	最新の12.1Eへの移行	
12.0XT	脆弱性あり。TACに連絡	
12.0XU	脆弱性あり。TACに連絡	
12.0XV	12.1以降に移行	
該当する 12.1 ベースのリリース	リビルド	メンテナンスリリース
12.1		12.1(26)
12.1AA	最新の12.2への移行が必要	
12.1AX	12.1(14)AX3	
12.1AY	12.1(22)EA2以降に移行	

12.1AZ	12.1(22)EA2以降に移行	
12.1DA	脆弱性あり。TACに連絡	
12.1DB	12.3(4)T11以降に移行	
12.1DC	12.3(4)T11以降に移行	
12.1E	12.1(22)E3	
	12.1(23)E2	
		12.1(26)E
12.1EA	12.1(22)EA2	
12.1EC	脆弱性あり。TACに連絡	
12.1EO	脆弱性あり。TACに連絡	
12.1EV	最新の12.2Sに移行	
12.1EW	12.2(18)EW2以降に移行	
12.1EX	最新の12.1Eへの移行	
12.1EY	最新の12.1Eへの移行	
12.1T	12.2以降に移行	

12.1XA	12.2以降に移行	
12.1XB	12.2以降に移行	
12.1XC	12.2以降に移行	
12.1XD	12.2以降に移行	
12.1XE	最新の12.1Eへの移行	
12.1XF	12.3以降に移行	
12.1XG	12.3以降に移行	
12.1XH	12.2以降に移行	
12.1XI	最新の12.2への移行が必要	
12.1XJ	12.3以降に移行	
12.1XL	12.3以降に移行	
12.1XM	12.3以降に移行	
12.1XP	12.3以降に移行	
12.1XQ	12.3以降に移行	
12.1XR	12.3以降に移行	

12.1XT	12.3以降に移行	
12.1XU	12.3以降に移行	
12.1XV	脆弱性あり。TACに連絡	
12.1YA	12.3以降に移行	
12.1YB	12.3以降に移行	
12.1YC	12.3以降に移行	
12.1YD	12.3以降に移行	
12.1YE	12.3以降に移行	
12.1YF	12.3以降に移行	
12.1YH	12.3以降に移行	
12.1YI	12.2(2)YC以降に移行	
12.1YJ	12.1(22)EA2以降に移行	
該当する 12.2ベース	リビルド	メンテナンス リリース
12.2		12.2(27)
12.2B	12.3(4)T11以降に移行	

12.2BC	脆弱性あり。TACに連絡	
12.2BW	12.3以降に移行	
12.2BX	12.3(7)XI3への移行 –2005年2月15日から利用可能	
12.2BY	12.3(4)T11以降に移行	
12.2BZ	12.3(7)XI3への移行 –2005年2月15日から利用可能	
12.2CZ	脆弱性あり。TACに連絡	
12.2DA	脆弱性あり。TACに連絡	
12.2DD	12.3(4)T11以降に移行	
12.2DX	12.3(4)T11以降に移行	
12.2EW	12.2(18)EW2	
		12.2(25)EW
12.2JK	12.2(15)JK2	
12.2MB	12.2(25)SW以降に移行	
12.2MC	12.3(11)T以降に移行	

12.2MX	12.3(8)T5以降に移行	
12.2S		12.2(25)S
	12.2(14)S13	
	12.2(18)S8	
	12.2(20)S7	
12.2SE	12.2(20)SE3	
12.2SU	12.2(14)SU2	
12.2SW	12.2(25)SWに移行	
12.2SX	12.2(17d)SXB5に移行	
12.2SXA	12.2(17d)SXB5に移行	
12.2SXB	12.2(17d)SXB5	
12.2SXD	12.2(18)SXD2	
12.2SY	12.2(17d)SXB5に移行	
12.2SZ	12.2(25)S以降に移行	
12.2T	12.2(15)T15	

12.2XA	12.3以降に移行	
12.2XB	12.3以降に移行	
12.2XC	12.3以降に移行	
12.2XD	12.3以降に移行	
12.2XE	12.3以降に移行	
12.2XF	脆弱性あり。TACに連絡	
12.2XG	12.3以降に移行	
12.2XH	12.3以降に移行	
12.2XI	12.3以降に移行	
12.2XJ	12.3以降に移行	
12.2XK	12.3以降に移行	
12.2XL	12.3以降に移行	
12.2XM	12.3以降に移行	
12.2XN	12.3以降に移行	
12.2XQ	12.3以降に移行	

12.2XS	12.3以降に移行	
12.2XT	12.3以降に移行	
12.2XU	12.3以降に移行	
12.2XW	12.3以降に移行	
12.2XZ	12.3以降に移行	
12.2YA	12.2(4)YA8	
12.2YB	12.3以降に移行	
12.2YC	12.3以降に移行	
12.2YE	12.2S以降に移行	
12.2YF	12.3以降に移行	
12.2YG	12.3以降に移行	
12.2YH	12.3以降に移行	
12.2YJ	12.3以降に移行	
12.2YK	12.3T以降に移行	
12.2YL	12.3T以降に移行	

12.2YM	12.3T以降に移行	
12.2YN	12.3T以降に移行	
12.2YO	12.2(17d)SXB5に移行	
12.2YP	12.3以降に移行	
12.2YQ	12.3(4)T11以降に移行	
12.2YR	12.3(4)T11以降に移行	
12.2YS	12.3T以降に移行	
12.2YT	12.3以降に移行	
12.2YU	12.3T以降に移行	
12.2YV	12.3(4)T11以降に移行	
12.2YW	12.3(4)T11以降に移行	
12.2YX	12.2(14)SU2以降に移行	
12.2YY	12.3T以降に移行	
12.2YZ	12.2(25)S以降に移行	
12.2ZA	12.2(17d)SXB5または 12.2(18)SXD2への移行	

12.2ZB	12.3T以降に移行	
12.2ZC	12.3T以降に移行	
12.2ZD	12.3以降に移行	
12.2ZE	12.3以降に移行	
12.2ZF	12.3(4)T11以降に移行	
12.2ZG	12.3(4)T11以降に移行	
12.2ZH	12.3(4)T11以降に移行	
12.2ZI	12.2(25)S以降に移行	
12.2ZJ	12.3T以降に移行	
12.2ZK	12.2(15)ZK6	
12.2ZL	12.3(7)T7以降に移行	
12.2ZN	12.3T以降に移行	
12.2ZO	12.3以降に移行	
12.2ZP	脆弱性あり。TACに連絡	
該当する 12.3ベース	リビルド	メンテナンス リリース

12.3	12.3(6d)	
	12.3(9c)	
	12.3(10a)	
		12.3(12)
12.3B	12.3(5a)B3	
12.3BC	12.3(9a)BC1	
12.3BW	12.3(7)T7以降に移行	
12.3T	12.3(4)T11	
	12.3(7)T7	
	12.3(8)T5	
		12.3(11)T
12.3XA	12.3(7)T7以降に移行	
12.3XB	12.3(8)T5以降に移行	
12.3XC	12.3(2)XC3	
12.3XD	12.3(4)XD4	

12.3XE	12.3(2)XE1	
12.3XF	12.3(11)T以降に移行	
12.3XG	12.3(11)T以降に移行	
12.3XH	12.3(11)T以降に移行	
12.3XI	12.3(7)XI3:2005年2月15日に入手可能	
12.3XJ	脆弱性あり。TACに連絡	
12.3XK	脆弱性あり。TACに連絡	
12.3XL	脆弱性あり。TACに連絡	
12.3XN	脆弱性あり。TACに連絡	
12.3XQ	12.3(4)XQ1リリース日は未定	
12.3XR	脆弱性あり。TACに連絡	
12.3XS	12.3(7)XS2	
12.3XU	12.3(8)XU4	
12.3XV	12.3(11)T以降に移行	
12.3XX	12.3(8)XX1	

12.3YA	12.3(8)YA1	
12.3YC	脆弱性あり。TACに連絡	
12.3YD	脆弱性あり。TACに連絡	
12.3YE	12.3(4)T11以降に移行	
12.3YF	脆弱性あり。TACに連絡	
12.3YH	脆弱性あり。TACに連絡	
12.3YJ	脆弱性あり。TACに連絡	
12.3YL	脆弱性あり。TACに連絡	

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco 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やその公表は確認しておりません。

この脆弱性は、Cisco の社内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-20050126-bgp

改訂履歴

Revision	2005年	「ソフトウェアバージョンと修正

1.5	3月21日	」セクションのIOSリリースの表で、IOSソフトウェア12.2Tの利用可能な修正済みリリース情報を更新。
リビジョン 1.4	2005年2月9日	詳細セクションの変更と追加
リビジョン 1.3	2005年2月4日	「ソフトウェアバージョンおよび修正の変更」の表、要約、該当製品、および詳細のセクション。
リビジョン 1.2	2005年2月1日	12.2Sに追加されたリビルド
リビジョン 1.1	2005年1月29日	該当するIOS XRを追加。構文のマイナーな変更。12.2ZAの移行パスを修正。
リビジョン 1.0	2005年1月26日	初回公開リリース

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。