複数のIOSベースのシスコ製品におけるTCPの脆弱性

アドバイザリーID : cisco-sa-20040420-tcp-ios
CVE-2004-0230
初公開日 : 2004-04-20 21:00
バージョン 2.1 : 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

Transmission Control Protocol（TCP；伝送制御プロトコル）仕様(RFC793)の脆弱性は、外部の研究者によって発見されています。不正利用に成功すると、攻撃者は以前に公に議論されたよりもはるかに短い時間で確立されたTCP接続をリセットすることができます。アプリケーションによっては、接続が自動的に再確立されることがあります。それ以外の場合は、ユーザはアクションを繰り返す必要があります（たとえば、新しいTelnetまたはSSHセッションを開く）。攻撃されたプロトコルによっては、攻撃が成功すると、終端された接続以外にも別の影響が生じる場合があるため、これを考慮する必要があります。この攻撃方法は、デバイス（ルータ、スイッチ、コンピュータなど）で終了するセッションにのみ適用でき、デバイスを通過するセッション（ルータによってルーティングされる中継トラフィックなど）にのみ適用できません。さらに、この攻撃ベクトルは、データの整合性や機密性を直接損なうものではありません。

TCPスタックを含むすべてのシスコ製品がこの脆弱性の影響を受けます。

このアドバイザリは https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-iosで公開されており、Cisco IOS®ソフトウェアを実行するシスコ製品に適用されるこの脆弱性について説明しています。

Cisco IOSソフトウェアを実行しない製品に対するこの脆弱性に関するアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-noniosから入手できます。

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

TCPスタックを含む製品は、この脆弱性の影響を受けやすくなります。すべてのシスコ製品およびモデルが影響を受けます。この脆弱性の重大度は、TCPを使用するプロトコルとアプリケーションによって異なります。

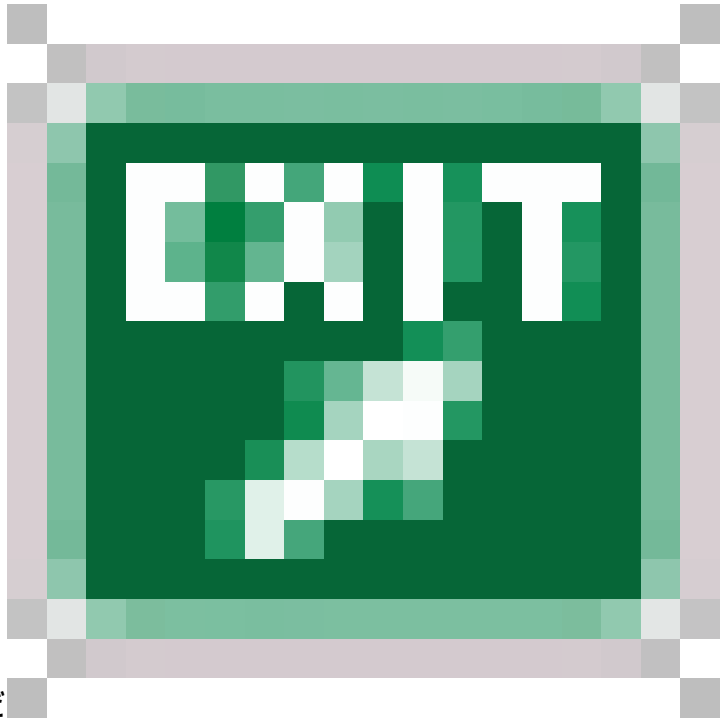
この攻撃方法は、デバイス（ルータ、スイッチ、コンピュータなど）で終了するセッションにのみ適用でき、デバイスを通過するセッション（ルータによってルーティングされる中継トラフィックなど）にのみ適用できません。

脆弱性を含んでいないことが確認された製品

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

TCPは、コネクション型の信頼性の高いデータストリーム配信を提供するように設計されたトランスポート層プロトコルです。これを実現するために、TCPは状態とシーケンス番号を示すフラグの組み合わせを使用して、パケットが再構成される順序を特定します。TCPは、確認応答番号と呼ばれる番号も提供します。この番号は、次に予想されるパケットのシーケンス番号を示すために使用されます。パケットのシーケンス番号が確認応答番号の範囲内（「ウィンドウ」と呼ばれます）にある場合にのみ、受信側のTCP実装によってパケットが再構成されます。リセットではパケットが返されることを予期しないため、確認応答番号(ACK)はリセット(RST)フラグが設定されたパケットでは使用されません。TCPプロトコルの詳細な仕様については、

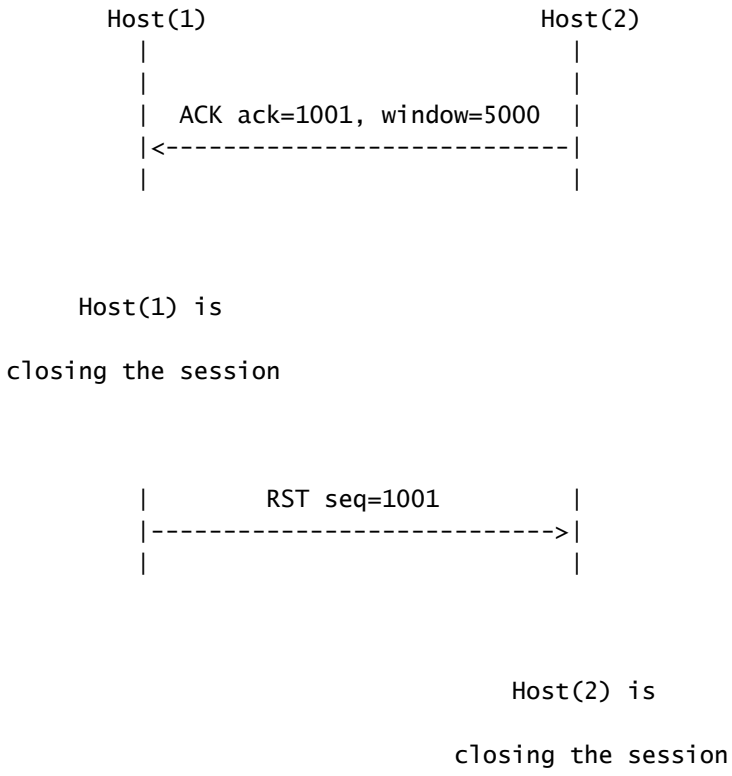


http://www.ietf.org/rfc/rfc0793.txtを参照してください。

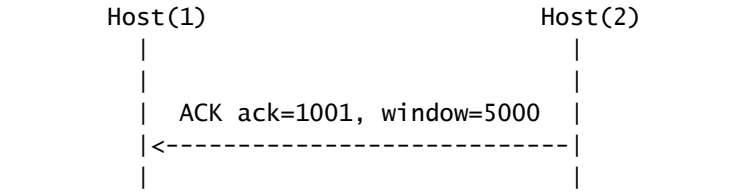
RFC793の仕様によると、RSTまたは同期(SYN)フラグが設定されたパケットを送信することで、確立されたTCP接続をリセットすることができます。これを行うには、4タプル（送信元と宛先の

IPアドレスとポート）がシーケンス番号とともに既知または推測されている必要があります。ただし、シーケンス番号は完全に一致している必要はなく、アドバタイズされたウィンドウ内に収まるのに十分です。これにより、相手が必要とする労力が大幅に軽減されます。ウィンドウが大きいほど、接続をリセットしやすくなります。送信元と宛先のIPアドレスは比較的簡単に判別できますが、送信元のTCPポートを推測する必要があります。宛先TCPポートは通常、すべての標準サービスで認識されています（たとえば、Telnetの場合は23、HTTPの場合は80）。Cisco IOSソフトウェアは、予測可能な増分の既知のサービスに予測可能な一時的なポートを使用します（後続の接続に使用される次のポート）。これらの値は、特定のCisco IOSソフトウェアバージョンおよびプロトコルでは一定ですが、リリースによって異なる場合があります。

TCPセッションの通常の終了の例を次に示します。



また、次のシナリオも許可されます。



2番目の例では、シーケンス番号(1001)が次に予想されたものではないにもかかわらず、RSTパケットがセッションを終了できることに注意してください。シーケンス番号は、アドバタイズされた「ウィンドウ」内に収まるのに十分でした。この例では、Host(2)は1001 ~ 6001のシーケンス番号を受け入れており、4321は明らかに許容範囲内にあります。

シスコは、http://www.watersprings.org/pub/id/draft-ietf-tcpm-tcpsecure-01.txtに従ってこの脆弱性を修正しました。

原則として、TCP接続が1分以上確立されたままになっているすべてのプロトコルは、公開されていると見なす必要があります。

この脆弱性に対するエクスポージャーは、次のように記述できます。

- Cisco IOS:Cisco IOSソフトウェアを実行しているすべてのデバイスに脆弱性が存在します。この脆弱性の影響を受けるのはセッションのエンドポイントのみであるため、デバイス自体で終了するTCPセッションのみが影響を受けます。デバイスを通過するセッションは、発信側または受信側デバイスが脆弱な場合にのみ脆弱ですが、ルータ自体で攻撃されることはありません。この脆弱性によってデータの整合性や機密性が損なわれることはありません。アベイラビリティにのみ影響します。
  この脆弱性は、Cisco Bug ToolkitにBug ID CSCed27956(登録ユーザ専用)およびCSCed38527(登録ユーザ専用)として文書化されています。
- Cisco IOS Firewall(IOS FW):Cisco IOS FWは、ルータ全体を通過するパケットを監視し、内部でセッション状態を維持します。このように、必要なポートを「オープン」してトラフィックを許可し、セッションが終了した後にトラフィックを閉じることができます。Cisco IOS FWはデバイスを通過するすべてのパケットを代行受信して検査するため、Cisco IOS FWを通過するすべてのTCPセッションがこの攻撃に対して脆弱です。これは、発信側デバイスと受信側デバイス自体に脆弱性がなくても有効です。
  この脆弱性は、Bug ID CSCed93836(登録ユーザ専用)としてCisco Bug Toolkitに記載されています。

- ネットワークアドレス変換(NAT)：この脆弱性はNATには影響しません。NAT機能は、ポートとIPアドレスを書き換えるだけです。この機能はTCPフラグを解釈しないため、この攻撃に対して脆弱ではありません。ただし、攻撃パケットはルータを通過し、受信側デバイスが影響を受ける可能性があります。

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。

Cisco IOS Firewallに対するこの脆弱性の影響を軽減する回避策はありません。

BGPの場合は、回避策といくつかの緩和策のみを示します。

- BGP MD5シークレット

  BGPの回避策は、ピア間の各セッションにMD5シークレットを設定することです。これは、次の例に示すように設定できます。

  <#root>

  ```
  router(config)#
  router bgp <AS-_number>
  router(config-router)#
  neighbor <IP_address> password <enter_your_secret_here>
  ```

  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、次のドキュメントhttp://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/1cbgp.htmlを参照してください。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統合されたCSCdx23494(登録ユーザ専用)修正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。

BGPセッションがファイアウォールを通過する場合は、TCPシーケンスのランダム化を無効にすることが重要です。ファイアウォールの中には、背後にあるホストを保護するためにTCPシーケンス番号を変更するものがあります。この機能を無効にしないと、BGPセッションは確立されず、次のエラーメッセージがルータのコンソールに表示されます。

```
%TCP-6-BADAUTH: Invalid MD5 digest from <peer1> to <peer2>
```

PIX Firewallを使用している場合は、次の例に示すように、コマンドにnorandomseqキーワードを追加します。

```
<#root>

static (inside,outside)

                netmask 255.255.255.0 norandomseq
```

この脆弱性に対しては、次の対策のうち1つ以上を適用することでBGPの危険性を軽減できます。これにより、攻撃の実装に必要なスプーフィングの可能性が低くなります。

- コアインフラストラクチャへのアクセスのブロック

  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アクセスコントロールリスト(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の回避策としてだけでなく、優れたネットワークセキュリティへの長期的な付加機能として考慮する必要があります。http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtmlで手できる『Protecting Your Core: Infrastructure Protection Access Control Lists』というホワイトペーパーには、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が記載されています。例外には、インフラストラクチャにアクセスする正当な理由があるデバイス（BGPピア、NTPソース、DNSサーバなど）が含まれます。その他のトラフィックはすべて、どのデバイスでも終端することなくネットワークを通過できる必要があります。

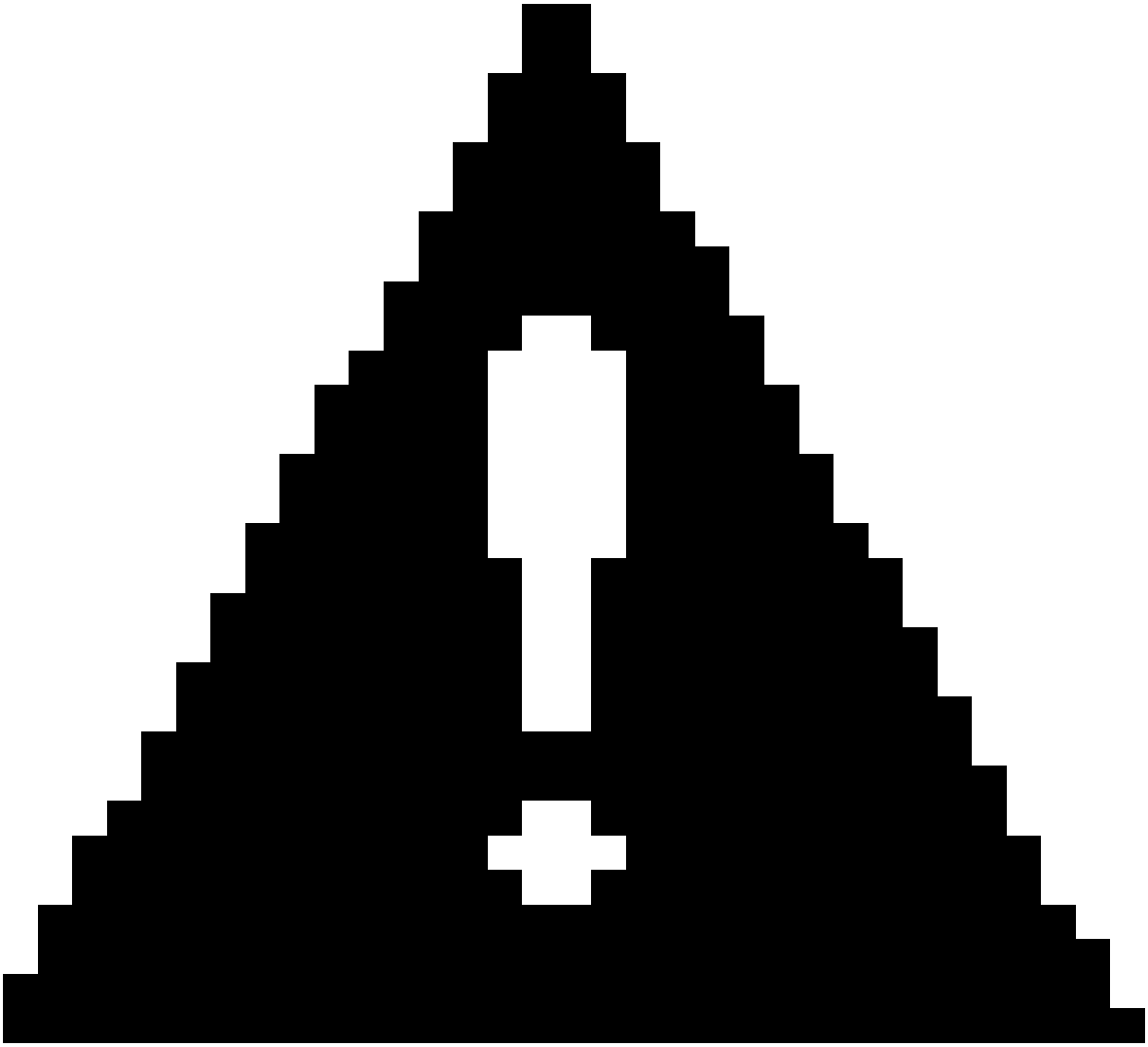
- ネットワークエッジでアンチスプーフィング対策を設定する

攻撃者がこのアドバイザリで説明されている攻撃ベクトルを使用するには、BGPピアの1つに等しい送信元IPアドレスを持つパケットを送信する必要があります。スプーフィングされたパケットは、Unicast Reverse Path Forwarding(uRPF)機能を使用するか、アクセスコントロールリスト(ACL)を使用してブロックできます。
uRPFを有効にすると、スプーフィングされたすべてのパケットは最初のデバイスでドロップされます。uRPFを有効にするには、次のコマンドを使用します。

```
<#root>

router(config)#

ip cef


router(config)#

interface
```

```
router(config-if)#

ip verify unicast reverse-path
```

uRPFの動作の詳細と、さまざまなシナリオでの設定方法については、http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.htmlおよびftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdfを参照してください。これは、非対称ルーティングを使用している場合に特に重要です。
また、ACLはできるだけエッジの近くに配置する必要があります。uRPFとは異なり、許可される正確なIP範囲を指定する必要があります。ブロックするアドレスを指定することは、維持が難しい傾向があるため、最適なソリューションではありません。



注意：アンチスプーフィング対策を効果的に行うには、保護されるデバイスから少なくとも1ホップ離れた場所にアンチスプーフィング対策を展開する必要があります。理想的には、お客様が直面しているネットワークエッジに導入されます。

- パケットレート制限
  Cisco IOSソフトウェアでは、RSTパケットはデフォルトでレート制限されています。この機能は、Cisco IOSソフトウェアリリース10.2で導入されました。RSTパケットのストームの場合、それらは実質的に1秒につき1パケットに制限されます。攻撃者が成功するには、最初のいくつかのパケットで接続を終了する必要があります。さもなければ、攻撃は実行不可能に長いと見なされます。一方、SYNパケットにはレート制限はありません。
  レート制限は、専用アクセスレート(CAR)またはコントロールプレーンポリシング(CPP)を使用して実行できます。CPPは推奨されるアプローチですが、Cisco IOSソフトウェアリリース12.2(18)Sおよび12.3(4)Tでのみ使用できます。現在、1751、2600/2600-XM、3700、7200、および7500シリーズのルータでのみサポートされています。
  CARは次のように設定できます。

```
<#root>

router(config)#

access-list 103 deny tcp any host 10.1.1.1 established


router(config)#

access-list 103 permit tcp any host 10.1.1.1


router(config)#

interface <interface> <interface #>


router(config-if)#

rate-limit input access-group 103 8000 8000 8000 conform-action transmit
exceed-action drop
```

CPPの設定および導入方法の詳細については、次のドキュメントを参照してください。
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900a

修正済みソフトウェア

シスコは2004年4月20日に複数のアドバイザリをリリースしました。

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は、修正を含む最初のリリースとそれぞれの提供予定日が「Rebuild」、「Interim」、および「Maintenance」の各列に表示されます。場合によっては、特定のリリースのリビルドが計画されていない場合があります。この場合、「Not scheduled」というラベルが付きます。 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
  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同じトレインで構築されており、特定の脆弱性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。シスコでは、この脆弱性に対処するためにメインラインストレインのリビルドを数種類提供していますが、最新のメンテナンスリリースのみをメインラインストレインで実行することを強く推奨します。

- Interim
  メンテナンスリリース間で定期的に構築され、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。暫定リリースは製品としては提供されず、通常は、Cisco Technical Assistance Center（TAC）によって事前に手配されない限り、CCO からダウンロードできません。

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、次の表に示すように、Cisco TACに連絡して支援を求めてください。

Cisco IOSファイアウォール用の修正済みCisco IOSソフトウェアイメージ

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 12.1 ベースのリリース	リビルド	暫定	メンテナンス
12.1	12.1(22c)		
12.1E	12.1(19)E7		
	12.1(13)E14		
該当する 12.2 ベースのリリース	リビルド	暫定	メンテナンス
12.2	12.2(21b)		
	12.2(23a)		

12.2T	12.2(11)T11		
	12.2(13)T12		
	12.2(15)T12		
該当する 12.3 ベースのリリース	リビルド	暫定	メンテナンス
12.3	12.3(5c)		
	12.3(6a)		
12.3T	12.3(4)T6（2004年5月31日に入手可能）		

修正済みCisco IOSソフトウェアリリースと移行パス

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 11.1 ベースのリリース	リビルド	暫定	メンテナンス
11.1	11.1脆弱性あり11.2 への移行が必要		
11.1AA	11.1AAに脆弱性があります。11.2Pに移行		
11.1CC	11.1CCに脆弱性が存在します。12.0 への移		

	行が必要		
該当する 11.2 ベースのリリース	リビルド	暫定	メンテナンス
11.2	11.2(26f) 2004年4月21日に入手可能		
11.2P	11.2(26)P6（2004年4月21日に入手可能）		
11.2SA	11.2(8.12)SA6		
該当する 11.3 ベースのリリース	リビルド	暫定	メンテナンス
11.3	11.3脆弱性あり12.0 への移行が必要		
	11.3(11b)T4 2004年4月21日に入手可能		
	11.3(11e) 2004年4月21日に入手可能		
該当する 12.0 ベースのリリース	リビルド	暫定	メンテナンス

12.0			12.0(28)
12.0DA	12.0DAに脆弱性があります。12.2DAに移行		
12.0DB	12.0DBに脆弱性が存在します。12.1DBに移行		
12.0DC	12.0DCに脆弱性があります。12.1DCへの移行		
12.0S	12.0(21)S8		
			12.0(27)S
	12.0(26)S2		
	12.0(16)S11		
	12.0(24)S5		
	12.0(25)S3		
	12.0(23)S6		
12.0SL	12.0SLが脆弱です。12.0(23)S6に移行		
12.0ST	12.0ST脆弱性あり。12.0(26)S2に移行		
12.0SX	12.0(25)SX4未ビルド – TACにお問い合わせください。		

12.0SZ	12.0SZに脆弱性が存在します。12.0(26)S2に移行		
12.0T	12.0Tに脆弱性があります。12.1 への移行が必要		
12.0W5	12.0(25)W5(27b)（2004年5月に入手可能）		
	12.0(28)W5(30)		
12.0WC	12.0(5)WC9a（2004年4月21日に入手可能）		
12.0WT	12.0(13)WTに脆弱性があります。エンジニアリング終了		
12.0WX	12.0(4)WXに脆弱性が存在します。12.0W5への移行が必要		
12.0XA	12.0(1)XAに脆弱性が存在します。最新の12.1への移行が必要		
12.0XB	12.0(1)XBに脆弱性が存在します。12.2(15)T12に移行		
12.0XC	12.0(2)XCに脆弱性が存在します。最新の12.1への移行が必要		
12.0XD	12.0(2)XDに脆弱性があります。最新の12.1への移行が必要		
12.0XE	12.0(7)XEに脆弱性があります。最新の		

	12.1Eへの移行
12.0XG	12.0(3)XGに脆弱性が存在します。最新の12.1への移行が必要
12.0XH	12.0(4)XHに脆弱性が存在します。12.1 への移行が必要
12.0XI	12.0(4)XIに脆弱性があります。12.1 への移行が必要
12.0XJ	12.0(4)XJに脆弱性があります。最新の12.1への移行が必要
12.0XK	12.0(7)XKに脆弱性があります。最新の12.1Tへの移行
12.0XL	12.0(4)XL脆弱性あり。最新の12.2への移行が必要
12.0XM	12.0(4)XMに脆弱性があります。12.2(15)T12に移行
12.0XN	12.0(5)XNに脆弱性があります。最新の12.1への移行が必要
12.0XP	12.0(5.1)XPに脆弱性があります。12.0(5)WC9aに移行
12.0XQ	12.0(5)XQに脆弱性が存在します。最新の12.1への移行が必要
12.0XR	12.0(7)XRに脆弱性があります。最新の

	12.2への移行が必要		
12.0XS	12.0(5)XSに脆弱性があります。最新の12.1Eへの移行		
12.0XU	12.0(5)XUに脆弱性があります。12.0(5)WCへの移行		
12.0XV	12.0(7)XVに脆弱性が存在します。12.2(15)T12に移行		
該当する12.1 ベースのリリース	リビルド	暫定	メンテナンス
12.1	12.1(20a)		
	12.1(4c)		
	12.1(22b) IOS FW修正なし		
	12.1(22c)（IOS FW修正あり）		
12.1AA	12.1(10)AAに脆弱性があります。最新の12.2への移行が必要		
12.1AX	12.1(14)AX		
12.1AY	12.1(13)AY脆弱性あり12.1EAに移行		

12.1DA	12.1DA脆弱性12.2DAへの移行		
12.1DB	12.1(5)DBに脆弱性が存在します。12.2Bへの移行が必要		
12.1E	12.1(19)E7		
	12.1(22)E1		
	12.1(11b)E14		
	12.1(20)E2		
	12.1(19)E6		
	12.1(13)E13（IOS FW修正なし）		
	12.1(8b)E18		
	12.1(14)E10		
	12.1(13)E14（IOS FW修正あり）		
12.1EA	12.1(19)EA1b（Catalyst 3560のみ）		
	12.1(19)EA1c（Catalyst 2940、2950、2950-LRE、2955、2970、3550、3560、および3750）		

12.1EB	12.1(20)EB		
12.1EC	12.1(20)EC		
12.1EO	12.1(20)EO		
	12.1(19)EO2 2004年4月25日に提供開始		
12.1EU	12.1(20)EU		
12.1EV	12.1(12c)EVに脆弱性があります。 12.2(RLS4)Sに移行		
12.1EW	12.1(20)EW2		
12.1EX	12.1EXに脆弱性があります。12.1(14)Eに移行		
12.1EY	12.1(10)EYに脆弱性があります。 12.1(14)Eに移行		
12.1T	12.1(5)T17		
12.1XA	12.1(1)XAに脆弱性が存在します。 12.1(5)T18に移行		
12.1XB	12.1(1)XBに脆弱性が存在します。 12.2(15)T12に移行		
12.1XC	12.1(1)XCに脆弱性が存在します。12.2 への移行が必要		

12.1XD	12.1(1)XDに脆弱性があります。12.2 への移行が必要
12.1XE	12.1(1)XEに脆弱性が存在します。最新の12.1Eへの移行
12.1XF	12.1(2)XFに脆弱性が存在します。12.2(15)T12に移行
12.1XG	12.1(3)XGに脆弱性が存在します。12.2(15)T12に移行
12.1XH	12.1(2a)XHに脆弱性が存在します。12.2 への移行が必要
12.1XI	12.1(3a)XI脆弱性あり最新の12.2への移行が必要
12.1XJ	12.1(3)XJに脆弱性があります。12.2(15)T12に移行
12.1XL	12.1(3)XL脆弱性あり。最新の12.2Tへの移行
12.1XM	12.1(5)XMに脆弱性があります。最新の12.2Tへの移行
12.1XP	12.1(3)XPに脆弱性があります。12.2(15)T12に移行
12.1XQ	12.1(3)XQに脆弱性が存在します。最新の12.2Tへの移行
12.1XR	12.1(5)XRに脆弱性が存在します。最新の

	12.2Tへの移行
12.1XT	12.1(3)XTに脆弱性があります。 12.2(15)T12に移行
12.1XU	12.1(5)XUに脆弱性があります。最新の 12.2Tへの移行
12.1XV	12.1(5)XVに脆弱性が存在します。12.2XBに移行
12.1YA	12.1(5)YAに脆弱性があります。12.2(8)Tに移行
12.1YB	12.1(5)YBに脆弱性あり。12.2(15)T12に移行
12.1YC	12.1(5)YC脆弱性あり。12.2(15)T12に移行
12.1YD	12.1(5)YDに脆弱性があります。12.2(8)Tに移行
12.1YE	12.1(5)YE5に脆弱性があります。 12.2(2)YCに移行
12.1YF	12.1(5)YF2に脆弱性が存在します。 12.2(2)YCに移行
12.1YH	12.1(5)YH2に脆弱性があります。 12.2(13)Tに移行
12.1YI	12.1(5)YI2に脆弱性が存在します。 12.2(2)YCに移行

12.1YJ	12.1(11)YJに脆弱性があります。最新の12.1EAへの移行		
該当する 12.2 ベースのリリース	リビルド	暫定	メンテナンス
12.2	12.2(19b)		
	12.2(16f)		
	12.2(21a)		
			12.2(23)
	12.2(12i)		
	12.2(10g)		
	12.2(13e)		
	12.2(17d)		
	12.2(21b)		
	12.2(23a)		
12.2B	12.2(2)B - 12.2(4)B7に脆弱性があります。12.2(13)T12に移行		

	12.2(4)B8およびFWDに脆弱性が存在します。12.3(5a)B1に移行		
12.2BC	12.2(15)BC1C		
12.2BW	12.2(4)BWに脆弱性が存在します。 12.2(15)T12に移行		
12.2BX	12.2(16)BX3 5月中旬から利用可能		
12.2BY	12.2(4)BY Vulnerable」を参照してください。12.2(15)Bに移行		
	12.2(8)BY Vulnerable」を参照してください。12.2(8)ZBに移行		
	12.2(2)BY Vulnerable」を参照してください。12.2(8)BZに移行		
12.2BZ	12.2(15)BZに脆弱性が存在します。 12.2(16)BXに移行		
12.2CX	12.2(11)CXに脆弱性が存在します。 12.2(15)BCに移行		
12.2CY	12.2(11)CY脆弱性あり。12.2(13)BC1Cに移行		
12.2DA	12.2(12)DA6（2004年5月13日に入手可能）		
12.2DD	12.2DDに脆弱性があります。12.2(4)B1に移		

	行		
12.2DX	12.2(1)DXに脆弱性が存在します。12.2DDに移行		
	12.2(2)DXに脆弱性が存在します。最新の12.2Bへの移行が必要		
12.2EW	12.2(18)EW		
12.2JA	12.2(11)JA3		
	12.2(13)JA4		
	12.2(15)JA		
12.2MC	12.2(15)MC1B		
12.2S			12.2(22)S
	12.2(14)S7		
	12.2(20)S1		
	12.2(20)S3（2004年5月25日に入手可能）		
	12.2(18)S3		
12.2SE	12.2(18)SE		

12.2SW	12.2(21)SW		
12.2SX	12.2(17a)SX2（IOS FW修正なし）、12.2(17a)SX4（IOS FW修正あり）		
12.2SXA	12.2(17b)SXA2		
12.2SXB	12.2(17d)SXB1（IOS FW修正あり）		
	12.2(17d)SXB（IOS FW修正なし）		
12.2SY	12.2(14)SY3		
12.2SZ	12.2(14)SZ6		
12.2T	12.2(15)T11		
	IOS FW修正を含む 12.2(13)T12		
	12.2(11)T11 2004年4月26日に入手可能		
	12.2(13)T11（IOS FW修正なし）		
12.2XA	12.2(2)XAに脆弱性が存在します。 12.2(11)Tに移行		
12.2XB	12.2(2)XBに脆弱性が存在します。12.3 への移行が必要		

12.2XC	12.2(2)XCに脆弱性が存在します。 12.2(8)ZBに移行
12.2XD	12.2(1)XDに脆弱性があります。 12.2(15)T12に移行
12.2XE	12.2(1)XEに脆弱性が存在します。 12.2(15)T12に移行
12.2XF	12.2(1)XF1に脆弱性が存在します。 12.2(4)BC1Cに移行
12.2XG	12.2(2)XGに脆弱性が存在します。 12.2(8)Tに移行
12.2XH	12.2(2)XHに脆弱性が存在します。 12.2(15)T12に移行
12.2XI	12.2(2)XI2に脆弱性が存在します。 12.2(15)T12に移行
12.2XJ	12.2(2)XJに脆弱性があります。 12.2(13)T12に移行
12.2XK	12.2(2)XKに脆弱性が存在します。 12.2(15)T12に移行
12.2XL	12.2(4)XL脆弱性あり。12.2(15)T12に移行
12.2XM	12.2(4)XMに脆弱性があります。 12.2(15)T12に移行
12.2XN	12.2(2)XNに脆弱性が存在します。

	12.2(11)Tに移行
12.2XQ	12.2(2)XQに脆弱性が存在します。 12.2(15)T12に移行
12.2XS	12.2(1)XSに脆弱性が存在します。 12.2(11)Tに移行
12.2XT	12.2(2)XTに脆弱性があります。12.2(11)Tに移行
12.2XU	12.2(2)XUに脆弱性があります。 12.2(15)T12に移行
12.2XW	12.2(4)XWに脆弱性が存在します。 12.2(13)T12に移行
12.2YA	12.2(4)YAに脆弱性があります。 12.2(15)T12に移行
12.2YB	12.2(4)YBに脆弱性が存在します。 12.2(15)T12に移行
12.2YC	12.2(2)YC脆弱性あり。12.2(11)T11に移行
12.2YD	12.2(8)YDに脆弱性があります。12.2(8)YYに移行
12.2YE	12.2(9)YE脆弱性あり12.2Sへの移行
12.2YF	12.2(4)YFに脆弱性あり。12.2(15)T12に移行

12.2YG	12.2(4)YGに脆弱性があります。 12.2(13)T12に移行
12.2YH	12.2(4)YHに脆弱性があります。 12.2(15)T12に移行
12.2YJ	12.2(8)YJに脆弱性があります。 12.2(15)T12に移行
12.2YK	12.2(2)YKに脆弱性があります。 12.2(13)ZCに移行
12.2YL	12.2(8)YLに脆弱性が存在します。12.3(2)Tに移行
12.2YM	12.2(8)YM脆弱性が存在します。12.3(2)Tに移行
12.2YN	12.2(8)YNに脆弱性があります。12.3(2)Tに移行
12.2YO	12.2(9)YOに脆弱性があります。 12.2(14)SYに移行
12.2YP	12.2(11)YPに脆弱性があります。最新の12.2Tへの移行
12.2YQ	12.2(11)YQに脆弱性が存在します。 12.3(2)Tに移行
12.2YR	12.2(11)YRに脆弱性あり。12.3(2)Tに移行
12.2YS	12.2(11)YS脆弱性あり12.3Tに移行

12.2YT	12.2(11)YTに脆弱性あり。12.2(15)Tに移行		
12.2YU	12.2(11)YUに脆弱性があります。12.3(2)Tに移行		
12.2YV	12.2(11)YVに脆弱性があります。12.3(4)Tに移行		
12.2YW	12.2(8)YWに脆弱性が存在します。 12.3(2)Tに移行		
12.2YX	12.2(11)YXに脆弱性があります。 12.2(RLS3)Sに移行		
12.2YY	12.2(8)YYに脆弱性があります。12.3(1)Tに移行		
12.2YZ	12.2(11)YZに脆弱性があります。 12.2(14)SZに移行		
12.2ZA	12.2(14)ZA6		
12.2ZB	12.2(8)ZBに脆弱性が存在します。12.3Tに移行		
12.2ZC	12.2(13)ZCに脆弱性が存在します。12.3Tに移行		
12.2ZD	12.2(13)ZD1		
12.2ZE	12.2(13)ZE脆弱性12.3 への移行が必要		

12.2ZF	12.2(13)ZFに脆弱性が存在します。 12.3(4)Tに移行		
12.2ZG	12.2(13)ZGに脆弱性が存在します。 12.3(4)Tに移行		
12.2ZH	12.2(13)ZHに脆弱性が存在します。 12.3(4)Tに移行		
12.2ZI	12.2(11)ZIに脆弱性があります。12.2(18)Sに移行		
12.2ZJ	12.2(15)ZJ5		
	12.2(15)ZJ4		
12.2ZK	12.2(15)ZKに脆弱性が存在します。12.3Tに移行		
12.2ZL	12.2(15)ZLに脆弱性が存在します。 12.3(7)Tに移行		
12.2ZN	12.2(15)ZNに脆弱性があります。12.3(2)Tに移行		
12.2ZP	12.2(13)ZP3		
該当する 12.3 ベースのリリース	リビルド	暫定	メンテナンス
12.3	12.3(3e)		

			12.3(6)
	12.3(5b)		
12.3B	12.3(5a)B		
	12.3(3)B1		
12.3BW	12.3(1a)BWに脆弱性が存在します。12.3Bへの移行が必要		
12.3T	12.3(2)T4		
	12.3(7)T1（2004年4月26日に入手可能）		
	12.3(4)T3		
	12.3(4)T6 With IOS FW fix、2004年5月31日に入手可能		
12.3XA	12.3(2)XAに脆弱性が存在します。TACにお問い合せください。		
12.3XB	12.3(2)XB2		
12.3XC	12.3(2)XC2		
12.3XD	12.3(4)XD1		
12.3XE	12.3(2)XEに脆弱性が存在します。12.3Tに移行		

12.3XF	12.3(2)XFに脆弱性が存在します。必要に応じてTACに連絡してください。		
12.3XG	12.3(4)XG		
12.3XH	12.3(4)XH		
12.3XI	12.3(7)XIに脆弱性があります。12.3Tに移行		
12.3XJ	12.3(7)XJに脆弱性が存在します。必要に応じてTACに連絡する		
12.3XK	12.3(4)XK		
12.3XL	12.3(7)XL脆弱性あり。必要に応じてTACに連絡する		
12.3XM	12.3(9)XMに脆弱性があります。必要に応じてTACに連絡してください。		
12.3XN	12.3(4)XNに脆弱性が存在します。必要に応じてTACに連絡してください。		
12.3XQ	12.3(4)XQに脆弱性が存在します。必要に応じてTACに連絡してください。		

*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

この脆弱性は公開カンファレンスで報告されました。Cisco PSIRTでは、このアドバイザリに記載されている脆弱性の不正利用の可能性は確認していません。

RSTフラグが設定されたパケット（リセットパケット）に関する脆弱性の不正利用は、OSVDB.orgのPaul (Tony) Watson氏によって発見されました。攻撃ベクトルがSYNフラグを持つパケットに拡張されていることは、この問題の解決に協力しているベンダーによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-ios

改訂履歴

Revision 2.1	2005年4月13日	詳細セクションのリンク切れを修正。
Revision 2.0	2004年7月14日	修正済みCisco IOSソフトウェアリリースと移行パスの表を12.0SLのリビジョンで更新。
Revision 1.9	2004年6月16日	修正済みCisco IOSソフトウェアリリースと移行パスの表を、セクション12.0Sの新しい行で更新
リビジョン 1.8	2004年5月20日	ステータスが最終に変更されました。
Revision 1.7	2004年5月10日	12.0(28)、12.0(27)S、12.2(23)、12.2(22)S、12.3(6)、および12.2JAのCisco IOSファイアウォー

		ルの修正済みCisco IOSソフトウェアイメージのテーブルメンテナンスリビジョンを更新。
Revision 1.6	2004年5月4日	「ソフトウェアバージョンと修正」セクションで、12.0W5および12.2SXのエントリを更新。BGP MD5シークレットに関する情報を含む「回避策」セクションを更新。
Revision 1.5	2004年4月30日	「ソフトウェアバージョンと修正」セクションで、12.1、12.3T FW、および12.1DAのエントリを更新。12.3T IOSメインおよび12.2ベースのリリースに新しいセクションを追加。
リビジョン 1.4	2004年4月28日	「詳細」セクションで、DoDドラフトTCPプロトコルへのリンクを追加しました。 「不正利用と公表」セクションで、最初の文の文言を変更。
リビジョン 1.3	2004年4月25日	「ソフトウェアバージョンと修正」セクションに、アドバイザリ付きの導入パラグラフを追加。 「ソフトウェアバージョンと修正」セクションで、エントリ12.1AY、12.2BX、12.2XB、12.2T、および12.2SXBに関するCisco IOSソフトウェアリリースと移行パスの表を更新。 「回避策」セクションで、「ネットワークエッジエントリでアンチスプーフィング対策を設定する」のコマンドシーケンスを更新。

リビジョン 1.2	2004年4月22日	「ソフトウェアバージョンと修正」セクションで、12.1Eエントリに関するCisco IOS Firewallの表を更新。 「ソフトウェアバージョンと修正」セクションで、エントリ12.2SXA、12.2SXB、12.1EW、12.2S、12.3T、12.2JA、12.1EAに関するCisco IOSソフトウェアリリースと移行パスの表を更新。
リビジョン 1.1	2004年4月21日	「ソフトウェアバージョンと修正」セクションのCisco IOSソフトウェアリリースと移行パスの表で、12.1(20)E2エントリを更新。 「ソフトウェアバージョンと修正」セクションの「Cisco IOSソフトウェアリリースと移行パスの表、12.1E」セクションで、12.1(13)E13エントリを更新。 「ソフトウェアバージョンと修正」セクションの「Cisco IOSソフトウェアリリースと移行パスの表、12.1E」セクションで、12.1(13)E14エントリを更新。 「ソフトウェアバージョンと修正」セクションの「Cisco IOSソフトウェアリリースと移行パスの表、12.2T」セクションで、12.2(13)T12エントリを更新。 「ソフトウェアバージョンと修正」セクションの「Cisco IOSソフトウェアリリースと移行パスの表、12.2T」セクションで、12.2(13)T11エントリを更新。 「回避策」セクションの「パケットレート制限」サブセクションを次の

		行に更新：access-list 103 permit tcp any host 10.1.1.1
リビジョン 1.0	2004年4月20日	初回公開リリース

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。