# IOS以外の複数のシスコ製品におけるTCPの脆弱性

Medium

アドバイザリーID : cisco-sa-20040420-tcp-nonios
CVE-2004-0230
初公開日 : 2004-04-20 21:00
最終更新日 : 2014-10-23 12:53
バージョン 2.1 : Final
CVSSスコア : 5.0
回避策 : No Workarounds available
Cisco バグ ID : CSCuq38097

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、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-nonios で公開されており、Cisco IOS®ソフトウェアを実行しない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する製品の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-ios で入手できます。

# 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。

場合によっては、脆弱性は基盤となるオペレーティングシステムにあります。このような場合、パッチの提供は元のOSベンダーに依存します。

脆弱性が存在するIOSベース以外のシスコ製品の一覧は次のとおりです。

- アクセス レジストラ
- BPX 8600、IGX 8400、MGX 82xx、88xxおよび8950 WANスイッチ、およびService Expansion Shelf
- BR340、WGB340、AP340、AP350、BR350 Cisco/Aironetワイヤレス製品
- Cache Engine 505および570
- CallManager
- Catalyst 1200、1900、28xx、2948G-GE-TX、3000、3900、4000、5000、6000
- Cisco 8110ブロードバンドネットワーク終端ユニット
- Cisco Element Managementフレームワーク
- Cisco Info Center
- Cisco Intelligent Contact Management(ICM)
- Cisco MDS 9000
- Cisco ONS 15190/15194 IP Transportコンセントレータ
- Cisco ONS 15327メトロエッジオプティカルトランスポートプラットフォーム
- Cisco ONS 15454オプティカルトランスポートプラットフォーム
- Cisco ONS 15531/15532 T31 OMS Metro WDMシステム
- Cisco ONS 15800/15801/15808 Dense Wave Division Multiplexing Platform
- Cisco ONS 15830 T30 Optical Amplificationシステム
- Cisco ONS 15831/15832 T31 DWDMシステム
- Cisco ONS 15863 T31 Submarine WDMシステム
- Content Router 4430およびContent Delivery Manager 4630および4650
- CiscoSecure ACS for Windows and Unix、およびCiscoSecure ACS 1111アプライアンス
- Cisco Secure Intrusion Detection System(NetRanger)アプライアンスおよびIDSモジュール
- Cisco Secure PIXファイアウォール
- Cisco ws-x6608およびws-x6624 IPテレフォニーモジュール
- CiscoWorksウィンドウ

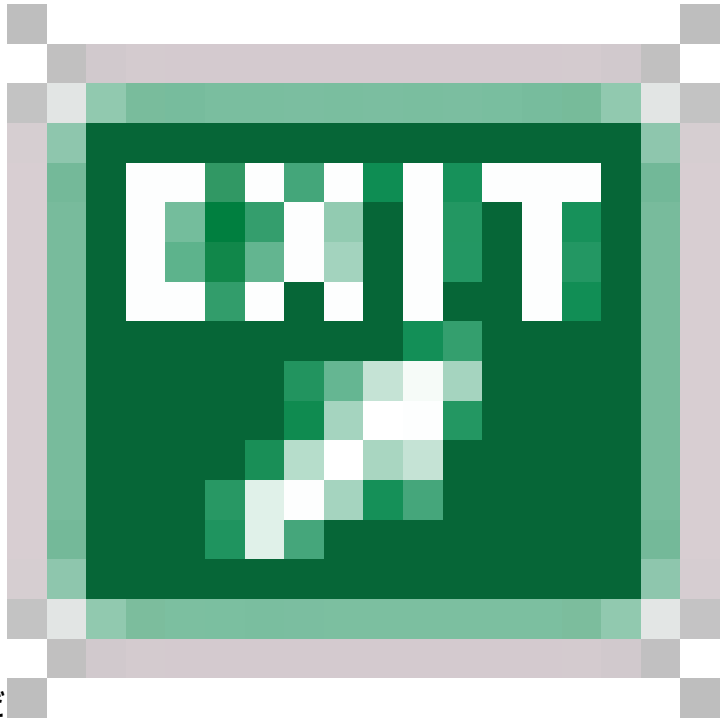
- Content Engine 507、560、590、および7320
- CSS11000(Arrowpoint)コンテンツサービススイッチ
- ホスティングソリューションエンジン
- User Registration Tool VLANポリシーサーバ
- Cisco FastHub 300および400
- CR-4430-B
- デバイス障害マネージャ
- Internet CDN Content Engine 590および7320、Content Distribution Manager 4670、Content Router 4450
- IP Phone（ATAおよびVG248を含むすべてのモデル）
- IP/TV
- LightStream 1010
- LightStream 100 ATMスイッチ
- LocalDirector
- ME1100シリーズ
- MicroHub 1500、MicroSwitch 1538/1548
- Voice Manager
- RTM
- SN5400シリーズストレージルータ
- スイッチプローブ
- Unity Server
- VG248 Analog Phone Gateway
- VPN5000 - VPNコンセントレータ
- トラフィックディレクタ
- WANマネージャ
- CSS 11050、CSS 11100、CSS 11150、CSS 11500およびCSS 11800
- GSS、CSM
- Cisco Channel Interface Processor(CIP)およびChannel Port Adapter(CPA)
- Cisco Systems ESCONチャネルポートアダプタ(ECPA)
- Cisco Systemsパラレルチャネルポートアダプタ(PCPA)
- Cisco Catalyst 6500シリーズおよびCisco 7600シリーズ(FWSM)用Cisco Firewall Services Module(FWSM)
- Cisco ACNS
- CiscoWorksワイヤレスLANソリューションアプライアンス
- Cisco VPN 3000 シリーズ コンセントレータ
- Cisco Standalone ラック サーバ CIMC

## 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

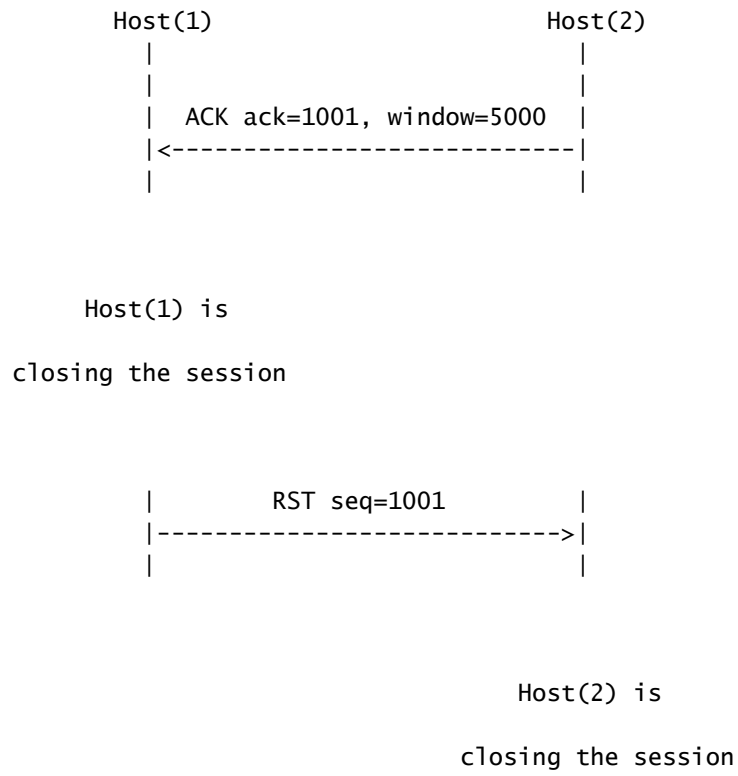
TCPは、コネクション型の信頼性の高いデータストリーム配信を提供するように設計されたトランスポート層プロトコルです。これを実現するために、TCPは状態とシーケンス番号を示すフラグの組み合わせを使用して、パケットが再構成される順序を特定します。TCPは、確認応答番号と呼ばれる番号も提供します。この番号は、次に予想されるパケットのシーケンス番号を示すために使用されます。パケットのシーケンス番号が確認応答番号の範囲内（「ウィンドウ」と呼ばれます）にある場合にのみ、受信側のTCP実装によってパケットが再構成されます。リセットではパケットが返されることを予期しないため、確認応答番号(ACK)はリセット(RST)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）。多くのオペレーティングシステム(OS)は、予測可能な増分で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（次の接続に使用される次のポート）。これらの値は、特定のOSやプロトコルでは一定ですが、OSのリリースによって異なります。

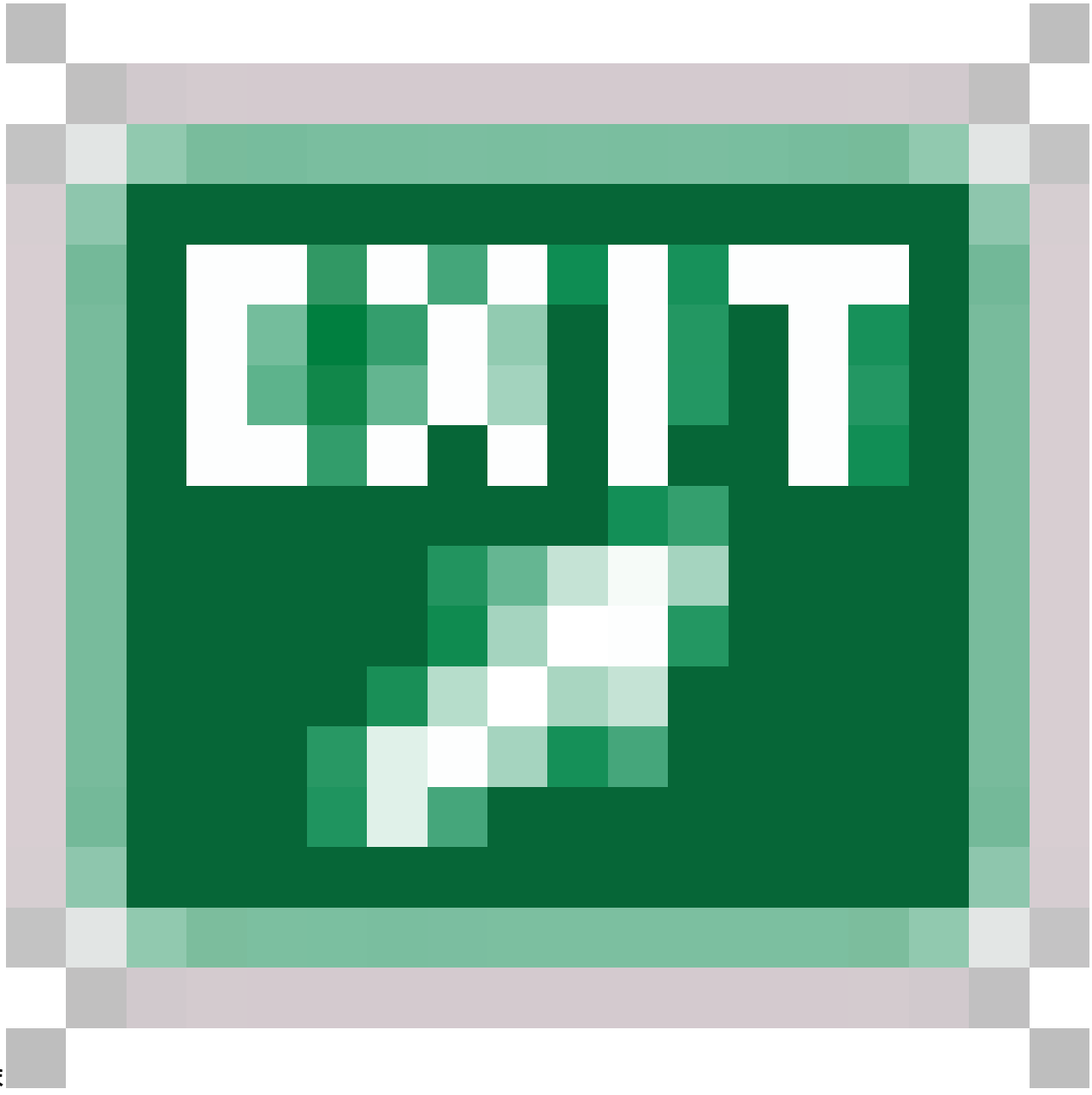
TCPセッションの通常の終了の例を次に示します。




また、次のシナリオも許可されます。

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.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-02.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。

## 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。

この脆弱性の影響を軽減する回避策はありません。

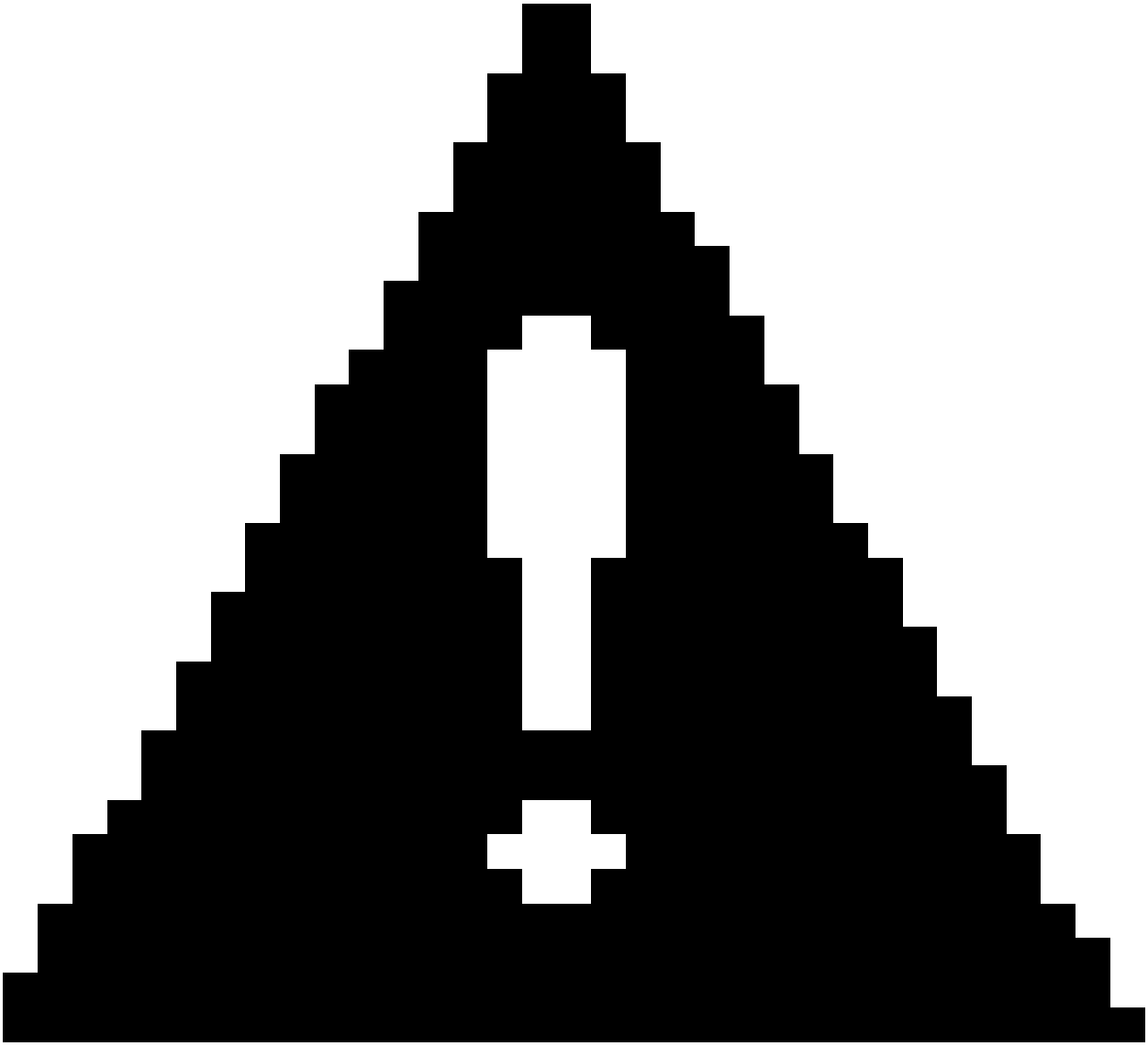
ネットワークのエッジにアンチスプーフィング機能を適用することで、この脆弱性の影響を緩和できます。

Unicast Reverse Path Forwarding(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。

アクセスコントロールリスト(ACL)も、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、ネットワークエッジに導入されます。

## 修正済みソフトウェア

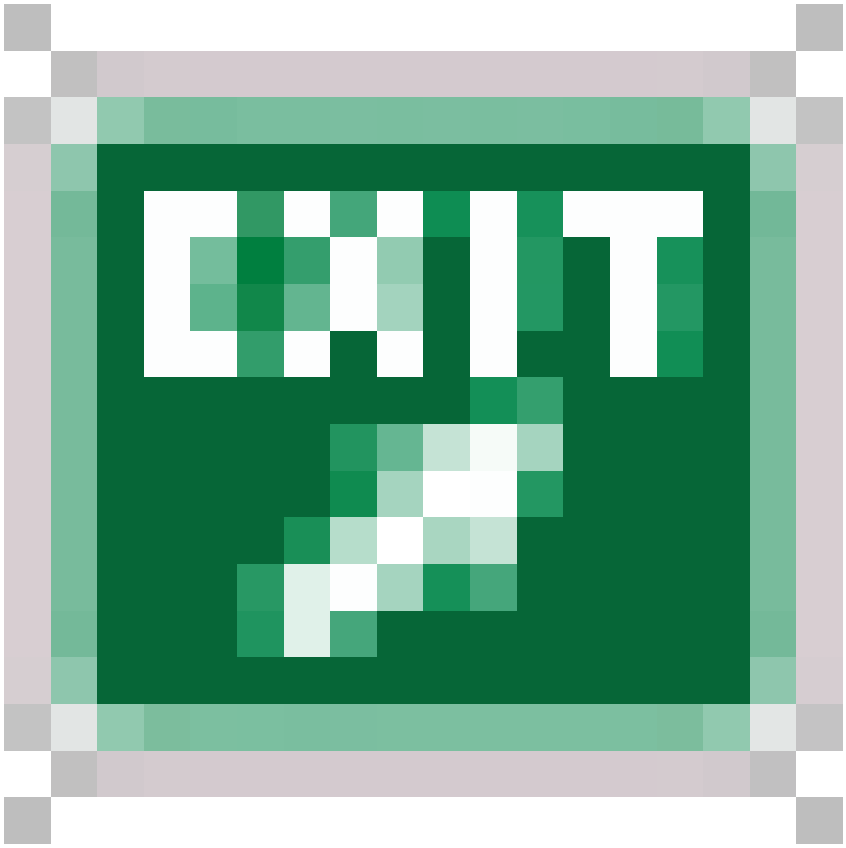
サードパーティ製のオペレーティングシステムをベースとするすべてのシスコ製品について、およびシスコからOSが提供されていない場合は、該当するパッチについて各ベンダーにお問い合わせください。

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。

| 製品 | 障害 ID | 最初の修正済みリリース |
|---|---|---|

| LAN スイッチング | | |
|---|---|---|
| Catalyst 1200、1900、28xx、29xx、3000、3900、4000、5000、6000 | CSCed32349(登録ユーザ専用) | 6.4(13)、6.4(12.3)、7.6(8.6)、8.3(2.8)、8.3(3.4)、8.4(0.47COC、8.4(0.91)COC、8.4(1.2)GLX、8.4(2.1)GLX、8.6(0.1)TAL、8.6(0.21)TAL |
| Catalyst 1900 および Catalyst 2820 | | 9.00.07 2004年4月27日に入手可能 |
| Catalyst 6500シリーズSSLサービスモジュール | CSCee35285(登録ユーザ専用) | 2.1(2) |
| ネットワークストレージ | | |
| Cisco MDS 9000ファミリ | CSCed27956(登録ユーザ専用)、CSCed38527(登録ユーザ専用)、CSCed65607(登録ユーザ専用) | 1.3(4a) |
| Ciscoチャネルインターフェイスプロセッサ(CIP) | CSCee35335(登録ユーザ専用) | 27-xおよび28-x、利用可能なソフトウェアなし。日付はまだ確定していませ |

| | | |
|---|---|---|
| | | ん。 |
| Cisco SN5428およびSN5428-2ストレージルータ | CSCee36193(登録ユーザ専用) | 3.5(3)-K9 |
| Unified Computing | | |
| Cisco Standalone ラック サーバ CIMC | CSCur03816(登録ユーザ専用) | 利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| 音声製品 | | |
| VG248 Analog Phone Gateway | CSCsk45124(登録ユーザ専用) | 利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| Catalyst 6500用のWS-6624 Analog Station Gateway Module | CSCee22691(登録ユーザ専用) | 利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| Windowsベースの CallManager | 修正：http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx | Windowsバージョン 2000.2.7sr5以降には修正プログ |

| | | |
|---|---|---|
| |  | ラムが含まれています |
| RedHatベースのCallManager | RedHatによる修正の提供を待っています | 利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| ワイヤレス製品 | | |
| Cisco Aironetアクセスポイント340、350、1200シリーズ（VxWorksベースのみ） | CSCee22526(登録ユーザ専用) | 利用可能なソフトウェアがありません。日付はまだ確定されていません。お客様にはIOSへの移行を推奨します。 |
| セキュリティ製品 | | |

| | | |
|---|---|---|
| シスコ侵入検知システム(IDS) | CSCee33732(登録ユーザ専用) | 5.0<br><br>利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| Cisco Catalyst 6500および7600シリーズ(FWSM)用Ciscoファイアウォールサービスモジュール | CSCee07453(登録ユーザ専用) | 1.1(3.17) TACへの問い合わせ |
| Cisco PIX ファイアウォール | CSCed31689(登録ユーザ専用)、CSCed91445(登録ユーザ専用)、CSCed70062(登録ユーザ専用)、CSCed91726(登録ユーザ専用) | 6.1.5(104)、6.2.3(110)、および6.3.3(133)のTACへのお問い合わせ |
| コンテント ネットワーキング | | |
| Cisco CSS11500ファミリ | CSCee06117(登録ユーザ専用)、SSLターミネーション | 07.30(00.09)S<br>07.20(03.10)S<br>07.30(00.08)S<br>07.10(05.07)S<br>07.20(03.09)S、<br>07.30(1.06)、<br>07.20(4.05) |
| Cisco CSS11000お | CSCee39336(登録ユーザ専用)、TCP管理接続 | 07.30(01.02)、<br>07.30(01.06)、 |

| | | |
|---|---|---|
| よび CSS11500ファミリ | | 07.20(04.05)、05.00(05.05)S、06.10(03.10)S |
| Ciscoコンテンツスイッチングモジュール(CSM) | CSCee33252(登録ユーザ専用) | 4.1(2) 2004年6月に入手可能、3.xリリースについてはTACにお問い合わせください。 |
| Cisco ACNS | CSCee37496(登録ユーザ専用) | 利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| Cisco 11000シリーズセキュアコンテンツアクセラレータ(SCA) | CSCee49634(登録ユーザのみ) | 利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| Cisco LocalDirector | CSCee08921(登録ユーザ専用) | 4.2(1)、4.2(2)、4.2(3)、4.2(4)、4.2(5)、4.2(6) |
| オプティカル製品 | | |
| Cisco ONS 15327、15454、および15454SDHオプティカル | CSCed73026(登録ユーザ専用) | R4.14は2004年4月27日に入手可能。今後のリリースはR4.62、R2.35。 |

| | | |
|---|---|---|
| トランスポートプラットフォーム | | |
| Cisco ONS 15501オプティカルトランスポートプラットフォーム | CSCee41687(登録ユーザ専用) | 利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| Cisco ONS 15600オプティカルトランスポートプラットフォーム | CSCed73026(登録ユーザ専用) | 今後のリリースR5.0 |
| WAN スイッチング | | |
| MGX 8850、MGX 8830、MGX 8950 | CSCee34615(登録ユーザ専用) | 4.0.17, 5.1.20, 5.2.00. |
| SES | CSCee34615(登録ユーザ専用) | 4.0.Xです。利用可能なソフトウェアがありません。日付はまだ確定されていません。 |
| MGX 8230、MGX 8250 | CSCee34620(登録ユーザ専用) | 1.2.23, 1.3.11. |
| MGX 8220 | この製品はサポート終了となっています。MGX 8230またはMGX 8250モデルにアップグレードすることをお勧めし | 修正済みソフトウェアは計画さ |

| | | |
|---|---|---|
| | ます。<br><br>http://www.cisco.com/en/US/products/hw/switches/ps1925/prod_eol_notice09186a00800a445d.html<br><br>CSCee34624(登録ユーザ専用) | れていません。 |
| BPX 8600、IGX 8400 | CSCee34625(登録ユーザ専用) | 9.3.51, 9.4.12 |
| VPNコンセントレータ | | |
| VPN 3000シリーズコンセントレータ | CSCsc28894(登録ユーザ専用) | 04.7.02.C<br><br>4.1.7.K. >リリース |

## 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フラグが設定され、データ注入が行われるパケットにまで拡大していることは、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-nonios

## 改訂履歴

| | | |
|---|---|---|
| リビジョ | 2014年10月23日 | CSCur03816、Ciscoスタンドアロンラックサーバ CIMCを追加。 |

| | | |
|---|---|---|
| ン<br>2.10 | | |
| 改訂<br>2.9 | 2008年1月<br>8日 | Cisco FWSM自体は影響を受けないため、CSCee07451とCSCee07450を削除しました。<br>MGXモデル8230、8250、8830、8850、および8950の修正済みソフトウェアリリースを追加。MGX 8220はサポートを終了しました。<br>BPX 8600およびIGX 8400の修正済みソフトウェアリリースを追加。 |
| 改訂<br>2.8 | 2007年<br>10月4日 | VG248に関する情報を追加。 |
| 改訂<br>2.7 | 2007年4月<br>3日 | CallMangerに関する情報を追加 |
| 改訂<br>2.6 | 2006年2月<br>14日 | VPN 3000シリーズコンセントレータの修正済みリリースのリストにリリース4.1.7.Kを追加。 |
| 改訂<br>2.5 | 2005-<br>December-<br>29 | 「Cisco VPN 3000シリーズコンセントレータ」を「該当製品」セクションに移動、「ソフトウェアバージョンと修正」セクションに「VPNコンセントレータ」を追加。 |
| 改訂<br>2.4 | 2004年<br>12月6日 | 詳細セクションのIETFドラフトへのリンクを変更。 |
| 改訂<br>2.3 | 2004年<br>12月3日 | 「ソフトウェアバージョンと修正」セクションの「コンテンツネットワーク」の見出しにCisco LocalDirectorの情報を追加。 |

| | | |
|---|---|---|
| 改訂<br>2.2 | 2004年<br>11月10日 | 「ソフトウェアバージョンと修正」セクションの表の最初の行 (「LANスイッチング」の下 ) を更新。 |
| 改訂<br>2.1 | 2004年<br>10月6日 | 「ソフトウェアバージョンと修正」セクションの「ネットワークストレージ」の見出しに、Cisco SN5428およびSN5428-2ストレージルータの情報を追加。 |
| 改訂<br>2.0 | 2004年9月<br>28日 | 「ソフトウェアバージョンと修正」セクションで、「セキュリティ製品」の下の表に次の行を追加しました。<br>Cisco Intrusion Detection System(IDS)5.0。ソフトウェアの入手可能日はまだ決定されていませCSCee33732。 |
| 改訂<br>1.9 | 2004年7月<br>7日 | 表の「コンテンツネットワーキング」の部分の「ソフトウェアバージョンと修正」セクションで、「Contact TAC」というテキストを削除し、最初の行に07.30(1.06)、07.20(4.05)を追加しました。<br>表の「Content Networking」のセクションの「Software Versions and Fixes」のセクションで、「No Software availability date has been determined yet.」というテキストを削除し、2行目に07.30(01.02)、07.30(01.06)、07.20(04.05)、05.00(05.05)S、06.10(03.10)Sを追加しました。 |
| 改訂 | 2004年6月 | 「ソフトウェアバージョンと修正」 |

| | | |
|---|---|---|
| 1.8 | 3日 | セクションに、Cisco 11000シリーズセキュアコンテンツアクセラレータ(SCA)のエントリを追加しました。 |
| 改訂<br>1.7 | 2004年5月<br>10日 | 「該当製品」セクションに、CiscoWorksワイヤレスLANソリューションアプライアンスを追加。「ソフトウェアバージョンと修正」セクションで、「LANスイッチング」の下に「Catalyst 6500シリーズSSLサービスモジュール」エントリを追加しました。 |
| 改訂<br>1.6 | 2004年5月<br>4日 | 「ソフトウェアバージョンと修正」セクションで、「セキュリティ製品」のPIXのエントリを更新。 |
| 改訂<br>1.5 | 2004年4月<br>30日 | 「ソフトウェアバージョンと修正」セクションで、「セキュリティ製品」のエントリを「PIX」に変更し、「オプティカル製品」のエントリを追加しました。 |
| 改訂<br>1.4 | 2004年4月<br>28日 | 「該当製品」セクションで、別の製品を追加し、該当しないリストから製品を移動しました。<br><br>「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。<br><br>「ソフトウェアバージョンと修正」セクションで、「セキュリティ製品とコンテンツネットワーキング」のエントリを更新。<br><br>「不正利用と公表」セクションで、最初の文の文言を変更。 |

| | | |
|---|---|---|
| 改訂<br>1.3 | 2004年4月<br>25日 | 「該当製品」セクションで、さらに製品をリストの最後に追加しました。<br><br>「ソフトウェアバージョンと修正」セクションに、アドバイザリとして導入パラグラフを追加。<br><br>「ソフトウェアバージョンと修正」セクションで、Cisco MDS 9000ファミリエントリを更新し、Cisco Channel Interface Processor(CIP)情報を追加。<br><br>「回避策」セクションで、uRPFを有効にするためにコマンドシーケンスを更新しました。 |
| 改訂<br>1.2 | 2004年4月<br>22日 | 「該当製品」セクションでBPXエントリを更新し、CiscoSecure ACS for Windows and UnixとCiscoSecure ACS 1111アプライアンスを追加しました。<br><br>「ソフトウェアバージョンと修正」セクションの表に「WANスイッチング」セクションを追加。 |
| 改訂<br>1.1 | 2004年4月<br>21日 | 「該当製品」セクション、更新されたCatalyst製品のリスト<br><br>「ソフトウェアバージョンと修正」セクションで、オプティカル製品が更新されました。<br><br>「ソフトウェアバージョンと修正」セクションで、セキュリティ製品が更新されています。 |
| 改訂 | 2004年4月 | 初回公開リリース |

| | | |
|---|---|---|
| 1.0 | 20日 | |

## 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。