Cisco Unified Communications Manager Express および Cisco IOS ソフトウェア H.323 および SIP DoS 脆弱性の識別し、軽減不正利用

Advisory ID: cisco-amb-20100324-voice

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100324-voice

リビジョン 1.1

一般公開 2010 年の 3 月に関しては 24 日 16:00 UTC（GMT）

目次

Cisco の対応

この応用軽減情報は次の PSIRT セキュリティ アドバイザリヘドキュメントガイドです:

- Cisco Unified Communications Manager Express Denial of Service（DoS/DDoS）脆弱性
- Cisco IOS ソフトウェア H.323 Denial of Service（DoS/DDoS）脆弱性
- Cisco IOS ソフトウェア Session Initiation Protocol（SIP） Denial of Service（DoS/DDoS）脆弱性

この資料は管理者がネットワーク デバイスを on Cisco 配置できる識別および軽減手法を提供したものです。

脆弱性の特性

Cisco IOS ソフトウェアに複数の脆弱性があります。 次のサブセクションはこれらの脆弱性を要約します:

Cisco Unified Communications Manager Express Denial of Service（DoS/DDoS）脆弱性: これらの脆弱性は認証とエンドユーザ 相互対話なしでリモートで不正利用することができます。 これらの脆弱性の正常な不正利用により影響を受けたデバイスはサービス拒否（DoS）状態という結果にクラッシュするか、または終りますかもしれません。 これらの脆弱性を不正利用する繰り返された試みは支えられた DoS 状態という結果に終る可能性があります。 不正利用のための不正侵

入ベクトルは TCPポート 2000 年を使用して Skinny Client Control Protocol （ SCCP ） パケットによってあります。

これらの脆弱性は CVE 識別 CVE-2010-0585 および CVE-2010-0586 を割り当てられました。

Cisco IOS ソフトウェア H.323 Denial of Service (DoS/DDoS) 脆弱性: これらの脆弱性は認証とエンドユーザ 相互対話なしでリモートで不正利用することができます。 これらの脆弱性の正常な不正利用により影響を受けたデバイスは DoS 状態という結果にクラッシュするか、または終りますかもしれません。 これらの脆弱性を不正利用する繰り返された試みは支えられた DoS 状態という結果に終る可能性があります。

不正利用のための不正侵入ベクターは次のプロトコルおよびポートを使用してパケットを通ってあります:

- TCPポート 1720 を使用する H.323
- TCPポート 2517 を使用する H.323

これらの脆弱性は CVE 識別 CVE-2010-0582 および CVE-2010-0583 を割り当てられました。

Cisco IOS ソフトウェア Session Initiation Protocol (SIP) Denial of Service (DoS/DDoS) 脆弱性: これらの脆弱性は認証とエンドユーザ 相互対話なしでリモートで不正利用することができます。 これらの脆弱性の正常な不正利用により影響を受けたデバイスは DoS 状態という結果にクラッシュするか、または終りますかもしれません。 これらの脆弱性を不正利用する繰り返された試みは支えられた DoS 状態という結果に終る可能性があります。

不正利用のための不正侵入ベクターは次のポートを使用してセッション開始プロトコル (SIP) パケットを通ってあります:

- TCPポート 5060
- TCPポート 5061
- UDP ポート 5060

攻撃者はスプーフィングされたパケットを使用して UDP ベース脆弱性を不正利用する可能性があります。

これらの脆弱性は CVE 識別 CVE-2010-0579、CVE-2010-0580 および CVE-2010-0581 を割り当てられました。

脆弱、変化しないについての情報は、および修正済みソフトウェア次のリンクで利用可能の PSIRT セキュリティ アドバイザリで利用できます:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-cucme
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-h323
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-sip

緩和テクニックの概要

Ciscoデバイスはこれらの脆弱性に複数の対策を提供します。 これらの保護方法は、インフラストラクチャ デバイスとネットワークを通過するトラフィックのセキュリティを保護する一般的な

ベスト プラクティスであると考えられます。 資料のこのセクションはこれらの手法の外観を提供します。

Cisco IOS ソフトウェアでは、次の方法を使用して、脆弱性の悪用を効果的に防止できます。

- インフラストラクチャ アクセスコントロール アクセス・コントロール・リスト（iACLs）
- Unicast Reverse Path Forwarding（ユニキャスト RPF）
- IP ソース ガード（IPSG）

これらの保護 メカニズム フィルタおよびドロップするは、またソース IP アドレスをの、これらの脆弱性を不正利用するように試みているパケット確認します。

ユニキャスト RPF の適切な配備および設定はスプーフィングされた出典 IP アドレスとパケットを使用する不正侵入に対して保護の有効な手段（方法）を提供します。 ユニキャスト RPF は、できるだけトラフィックの送信元の近くに配備する必要があります。

IPSG の適切な配備および設定はアクセス層でスプーフィング攻撃に対して保護の有効な手段（方法）を提供します。

また、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、Cisco PIX 500 シリーズ セキュリティ アプライアンス、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の Firewall Services Module（FWSM）でも、次のものを使用して、脆弱性の悪用を効果的に防止できます。

- 中継アクセスコントロール アクセス・コントロール・リスト（tACLs）
- アプリケ‐ションレイヤプロトコル インスペクション
- ユニキャスト RPF

これらの保護 メカニズム フィルタおよびドロップするは、またソース IP アドレスをの、これらの脆弱性を不正利用するように試みているパケット確認します。

Cisco Intrusion Prevention System（IPS; 侵入防御システム）のイベント アクションを有効に使用することで、この脆弱性を悪用しようとする攻撃の検出と防御が可能になります。

Cisco IOS NetFlow レコードはネットワークベース 不正利用試みに表示を提供できます。

Cisco IOS ソフトウェア、Cisco ASA および Cisco PIX セキュリティ アプライアンスおよび FWSM ファイアウォールは **show コマンド**からの出力で表示される syslog メッセージおよびカウンタ値によって可視性を提供できます。

リスク管理

組織はこれらの脆弱性の潜在的影響を判別するために標準リスク評価および軽減プロセスに従うように助言されます。 トリアージとは、プロジェクトを分類して、成功する可能性が高い取り組みに優先順位を付けることです。 Cisco では、各組織の情報セキュリティ チームがリスクベースのトリアージを行う能力を身に着けるために役立つドキュメントを提供しています。 セキュリティーの脆弱性 お知らせのためのリスク トリアージはおよびリスク トリアージおよびプロトタイピング反復可能な機密 保護 評価および応答プロセスを開発するために組織を助けることができます。

デバイス特有の軽減および識別

注意： あらゆる軽減手法の効果は製品ミックス、ネットワーク・トポロジ、交通現象および組織代表団のような特定の顧客 状況によって決まります。 設定を変更する際には、変更を適用する前にその設定の影響を評価する必要があります。

ここでは緩和策と識別策に関する情報が次のデバイス別に提供されています。

- Cisco IOS ルータおよびスイッチ
- Cisco IOS NetFlow
- Cisco ASA、PIX、および FWSM ファイアウォール

Cisco IOS ルータおよびスイッチ

緩和策： インフラストラクチャ アクセス コントロール リスト

インフラストラクチャ デバイスを保護し、リスクを、直接インフラストラクチャ不正侵入の影響最小限に抑えるためにおよび効果は、管理者 インフラストラクチャ 機器に送られるトラフィックのポリシー適用を行うためにインフラストラクチャ アクセスコントロール アクセス・コントロール・リスト（iACLs）を展開するように助言されます。 iACL は、既存のセキュリティ ポリシーと設定に基づいて、インフラストラクチャ デバイス宛ての正当なトラフィックのみを明示的に許可することによって構築されます。 インフラストラクチャ デバイスの保護を最大にするには、IP アドレスが設定されているすべてのインターフェイスの入力方向で配備済みの iACL を適用する必要があります。 iACL 回避策はこれらの脆弱性に対して不正侵入が信頼されたソース ソース・アドレスから起きるとき完全な保護を提供できません。

iACL ポリシーは影響を受けたデバイスに送信 されるポートおよび次の無許可のパケットを否定します:

- TCPポート 2000 年の SCCP パケット
- TCP ポート 1720 および 2517 の H.323 パケット
- TCP ポート 5060 および 5061 の SIP パケット
- UDP ポート 5060 の SIP パケット

次の例では、192.168.60.0/24 は影響を受けたデバイスによって使用する、192.168.100.1 のホストは影響を受けたデバイスへのアクセスを必要とする信頼されたソースとみなされます IP アドレス領域であり。 許可されないすべてのトラフィックを拒否する前に、ルーティングおよび管理アクセスに必要なトラフィックを許可するように注意する必要があります。 インフラストラクチャのアドレス レンジは、できるだけユーザおよびサービス セグメントに使用されるアドレス レンジとは別個にする必要があります。 このようにアドレスを設定することで、iACL の構築と配備が容易になります。

iACLs についての追加情報はコアの保護にあります: インフラストラクチャ保護 ACL』を参照してください。

```
 ip access-list extended Infrastructure-ACL-Policy
 ! !-- Include explicit permit statements for trusted sources !-- that require access on the
vulnerable ports ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2000 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 1720 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 2517 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 permit udp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5060 ! !-- The following vulnerability-specific access control entries !-- (ACEs)
```

```
can aid in identification of attacks ! deny tcp any 192.168.60.0 0.0.0.255 eq 2000 deny tcp any
192.168.60.0 0.0.0.255 eq 1720 deny tcp any 192.168.60.0 0.0.0.255 eq 2517 deny tcp any
192.168.60.0 0.0.0.255 eq 5060 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 deny udp any
192.168.60.0 0.0.0.255 eq 5060 ! !-- Explicit deny ACE for traffic sent to addresses configured
within !-- the infrastructure address space ! deny ip any 192.168.60.0 0.0.0.255 ! !-- Permit or
deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing security policies and
configurations ! !-- Apply iACL to interfaces in the ingress direction ! interface
GigabitEthernet0/0 ip access-group Infrastructure-ACL-Policy in
```

インターフェイス アクセス リストを使用してフィルタリングを行うと、ICMP 到達不能メッセージが、フィルタリングされたトラフィックの送信元に返されるようになります。 これらのメッセージを生成すると、デバイスの CPU 使用率が上昇する可能性があります。 Cisco IOS ソフトウェアでの ICMP 到達不能メッセージの生成は、デフォルトで 500 ミリ秒につき 1 パケットまでに制限されています。 ICMP 到達不能メッセージの生成を無効にするには、インターフェイス コンフィギュレーション コマンド **no ip unreachables** を使用します。 ICMP 到達不能レート制限をデフォルト設定から変更するには、グローバル コンフィギュレーション コマンド **ip icmp rate-limit unreachable** *interval-in-ms* を使用します。

緩和策： スプーフィング保護

Unicast Reverse Path Forwarding

この資料に説明があるいくつかの脆弱性はスプーフィングされたIP パケットによって不正利用することができます。 適切な配備および設定はの Unicast Reverse Path Forwarding（uRPF）次の脆弱性に関するスプーフィングに（ユニキャスト RPF）保護 メカニズムを提供できます:

- UDP パケットを使用する SIP Denial of Service（DoS/DDoS）脆弱性

ユニキャスト RPF はインターフェイス レベルで設定され、検証可能な送信元 IP アドレスを持たないパケットを検出して廃棄できます。 管理者はユニキャスト RPF にスプーフィングされたパケットがソース IP アドレス 存在にユニキャストによって RPF 有効に されるインターフェイスを通してネットワークに適切な帰りルート入るかもしれないので完全なスプーフィング保護を提供するために頼るべきではありません。 管理者はネットワークを通過している正当 な トラフィックを廃棄できるので適切なユニキャスト RPF モードが（緩くか厳密な）この機能の配備の間に設定されるようにする注意を奪取 するように助言されます。 エンタープライズ環境では、ユニキャスト RPF がインターネット エッジとレイヤ 3 インターフェイスの内部アクセス レイヤで有効になっている可能性があります。

追加情報は緩いモード 機能 ガイドに Unicast Reverse Path Forwarding（uRPF）あります。

ユニキャスト RPF の設定と使用についての詳細は、Applied Intelligence white paper『Unicast Reverse Path Forwarding について』を参照してください。

IP ソース ガード

IP ソース ガード（IPSG）は、非ルーテッド レイヤ 2 インターフェイス上の IP トラフィックを制限するため、DHCP スヌーピング バインディング データベースと、手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングするセキュリティ機能です。 IPSG を使用すると、送信元の IP アドレスや MAC アドレスを偽装することによってパケットをスプーフィングしようと試みる攻撃者からの攻撃を防止できます。 IPSG の適切な厳密なモード ユニキャスト RPF とつながれる配備および設定は次の脆弱性の軽減を助けるようにスプーフィング保護の最も有効な手段（方法）を提供できます:

- UDP パケットを使用する SIP Denial of Service（DoS/DDoS）脆弱性

IPSG の配備および設定についての追加情報は DHCP 機能および IP 出典ガードの設定にあります。

識別策： インフラストラクチャ アクセス コントロール リスト

管理者がインターフェイスに iACL を加えた後、**show ip access-lists コマンドは** iACL が適用するインターフェイスでフィルタリングされた特定のポートのパケットの数を確認します。 次のパケットおよびポートは識別されます:

- TCPポート 2000 年の SCCP パケット
- TCP ポート 1720 および 2517 の H.323 パケット
- TCP ポート 5060 および 5061 の SIP パケット
- UDP ポート 5060 の SIP パケット

フィルタリングされたパケットに対しては、これらの脆弱性を悪用しようとしていないかどうかを調査する必要があります。 次に **show ip access-lists Infrastructure-ACL-Policy** の出力例を示します。

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2000
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1720
    30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2517
    40 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    60 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
    70 deny tcp any 192.168.60.0 0.0.0.255 eq 2000 (6 matches)
    80 deny tcp any 192.168.60.0 0.0.0.255 eq 1720 (13 matches)
    90 deny tcp any 192.168.60.0 0.0.0.255 eq 2517 (10 matches)
    100 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (21 matches)
    110 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (11 matches)
    120 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (15 matches)
    130 deny ip any 192.168.60.0 0.0.0.255
router#
```

前の例では、アクセス リスト インフラストラクチャ ACL *ポリシー*は信頼できないホストかネットワークから受信される次のパケットを廃棄しました:

- ACE ラインのための 70 **TCPポート 2000 年の 6 つの SCCP** パケット
- ACE ラインのための 80 **TCPポート 1720 の H.323 13 の**パケット
- ACE ラインのための 90 **TCPポート 2517 の H.323 10 の**パケット
- ACE ラインのための 100 **TCPポート 5060 の 21 の SIP** パケット
- ACE ラインのための 110 **TCPポート 5061 の 11 の SIP** パケット
- ACE ラインのための 120 **UDP ポート 5060 の 15 の SIP** パケット

ACE カウンターおよび syslog イベントを使用して調査事件についての追加情報に関しては、ファイアウォールおよび IOS ルータ Syslog イベントによって加えられる知性 白書を使用して識別事件を参照して下さい。

管理者は特定の状態が満たされるとき見つかります組み込みイベント マネージャを ACE カウンターのような実装を提供するのに使用できます。 セキュリティ コンテキストの応用知性 白書によって組み込まれるイベント マネージャは方法についての追加詳細をこの機能を使用する提供します。

識別策： アクセス リスト ロギング

log および **log-input** アクセス コントロール リスト（ACL）オプションを使用すると、特定の ACE に一致するパケットがログに記録されます。 **log-input** オプションを使用すると、パケットの送信元および宛先の IP アドレスとポートに加え、入力インターフェイスのロギングが有効になります。

注意： アクセス コントロール リストのロギングは CPU に多大な負荷を与えることがあるので、使用する場合は細心の注意を払う必要があります。 ACL ロギングによる CPU への影響を左右する要素は、ログの生成、ログの送信、およびログが有効な ACE に一致するパケットを転送するプロセス交換です。

Cisco IOS ソフトウェアでは、**ip access-list logging interval** *interval-in-ms* コマンドを使用すると、ACL ロギングによって引き起こされるプロセス交換の影響を制限できます。 **logging rate-limit** *rate-per-second* [**except** *loglevel*] コマンドを使用すると、ログの生成と送信の影響を制限できます。

Supervisor Engine 720 または Supervisor Engine 32 を搭載した Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータでは、ACL ロギングによる CPU への影響をハードウェアで最適化することができます。

ACL ロギングの設定と使用についての詳細は、Applied Intelligence white paper『アクセス コントロール リストのログについて』を参照してください。

識別策： Unicast Reverse Path Forwarding を使用したスプーフィング保護

ネットワーク インフラストラクチャ全体展開され、正しく設定されてユニキャスト RPF が廃棄したパケットの数を確認するユニキャスト RPF が管理者は、**show ip interface 内部**使用できましたり、**show cef interface** *タイプ スロット/ポート* を **cef ドロップする**および **show ip traffic コマンドを示します**。

注: show コマンド | *regex* および **show コマンドを始めて下さい |** *regex* コマンド修飾子を望ましい情報を表示するために管理者が解析する必要がある出力の量を最小化するのに使用されています次の例で**含んで下さい**。 コマンド変更子についての追加情報は Cisco IOS設定の基礎 コマンド レファレンスの show コマンド セクションにあります。

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
    --      CLI Output Truncated       –
  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#
```

注: show cef interface *type slot/port* **internal** は、コマンドライン インターフェイスで省略なしに入力する必要がある非表示コマンドです。 このコマンドには、コマンド補完は使用できません。

```
router#show ip interface GigabitEthernet 0/0 | begin verify
    --      CLI Output Truncated       --
  IP verify source reachable-via RX, allow default, allow self-ping
  11 verification drops
  0 suppressed verification drops
router#
```

```
router#show cef drop
```

```
CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route      No_adj  ChkSum_Err
RP            27           0           0          18           0           0
router#


router#show ip traffic

IP statistics:
  Rcvd:  68051015 total, 2397325 local destination
         43999 format errors, 0 checksum errors, 33 bad hop count
         2 unknown protocol, 929 not a gateway
         21 security failures, 190123 bad options, 542768 with options
  Opts:  352227 end, 452 nop, 36 basic security, 1 loose source route
         45 timestamp, 59 extended security, 41 record route
         53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
         361634 other
  Frags: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 64666 received, 0 sent
  Mcast: 1589885 received, 2405454 sent
  Sent:  3001564 generated, 65359134 forwarded
  Drop:  4256 encapsulation failed, 0 unresolved, 0 no adjacency
         18 no route, 18 unicast RPF, 0 forced drop
         0 options denied
  Drop:  0 packets with source IP address zero
  Drop:  0 packets with internal loop back IP address
    --      CLI Output Truncated       --
router#
```

先行で **cef ドロップするを示せば show ip traffic** 例は、ユニキャスト RPF Cisco Express Forwarding（CEF）のフォワーディング情報ベース内の IP パケットの送信元アドレスを確認する不可能が理由でユニキャスト RPF が設定されているすべてのインターフェイスでグローバルに受信される **18 の IP パケットを**廃棄しました。

Cisco IOS NetFlow

識別策： NetFlow レコードを使用したトラフィック フローの識別

管理者はこれらの脆弱性を不正利用する試みであるかもしれないトラフィックフローの識別を援助するために Cisco IOS NetFlow IOS ルータおよびスイッチを on Cisco 設定できます。 管理者はこれらの脆弱性を不正利用する試みであるか、または正当 な トラフィックフローであるかどうか判別するためにフローを調査するために助言されます。

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
```

```
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP            236      0.0        12    66      0.0       1.8       4.8
TCP-FTPD            21      0.0     13726  1294      0.0      18.4       4.1
TCP-WWW          22282      0.0        21  1020      0.1       4.1       7.3
TCP-X              719      0.0         1    40      0.0       0.0       1.3
TCP-BGP              1      0.0         1    40      0.0       0.0      15.0
TCP-Frag         70399      0.0         1   688      0.0       0.0      22.7
TCP-other     47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS            582      0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.60.201  Gi0/1         192.168.60.102  11 0984 13C4     1
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 07D0     3
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    11 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 13C5     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   06 0B89 06B8     1
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.60.185  Gi0/1         192.168.60.239  11 4A89 13C4     4
Gi0/0         192.168.11.15   Gi0/1         192.168.60.239  06 5660 13C4     5
Gi0/0         192.168.12.165  Gi0/1         192.168.60.239  06 56BD 09D5     2
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
router#
```

前述の例では、**TCPポート 2000 年 (Hex 値 0x07D0)** の SCCP、TCP ポート 1720 （ **Hex 値 0x06B8)** および 2517 の **H.323 （ Hex 値 0x09D5)** および TCP ポート 5060 （ **Hex 値 0x13C4)** および **5061 （ Hex 値 0x13C5)** および UDP ポート 5060 （ **Hex 値 0x13C4)** の SIP のための複数のフローがあります。

UDP ポート 5060 の SIP パケットはからソースをたどられ、影響を受けたデバイスによって使用される 192.168.60.0/24 アドレスブロック内のアドレスに送信されます。 これらのフローのパケットはスプーフィングされ、これらの脆弱性を不正利用する試みを示すかもしれません。 管理者はまたこれらのフローを UDP ポート 5060 で送信 される SIP トラフィックのためのベースライン 利用と比較し、信頼できないホストかネットワークからソースをたどられるかどうか判別するためにすべてのフローを調査するために助言されます。

UDP ポート 5060 （ Hex 値 0x13C4 ）の SIP パケットのためのトラフィックフローだけ表示するため、コマンド **show ip cache flow | SrcIf|_11_.*13C4 を**表示しますここに示されているように関連 UDP NetFlow レコードを**含んで下さい**:

UDP フロー

```
router#show ip cache flow | include SrcIf|_11_.*13C4
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.60.10    Gi0/1         192.168.60.163  11 4203 13C4    56
Gi0/0         192.168.60.23    Gi0/1         192.168.60.20   11 4409 13C4    21
Gi0/0         192.168.60.13    Gi0/1         192.168.60.245  11 463F 13C4    13
router#
```

TCP ポート 5060 （ Hex 値 0x13C4 ）および 5061 の TCP ポート 1720 （ Hex 値 0x06B8 ）およ

び 2517 （Hex 値 0x9D5）および SIP パケットの TCPポート 2000 年（Hex 値 0x07D0）、H.323 パケットの SCCP パケットのためのトラフィックフローだけ表示するため（Hex 値 0x13C5）、コマンド **show ip cache flow | SrcIf|_06_.*(07D0|06B8|09D5|13C4|13C5)_ を**表示しますここに示されているように関連 TCP NetFlow レコードを**含んで下さい**:

TCP フロー

```
router#show ip cache flow | include SrcIf|_06_.*(07D0|06B8|09D5|13C4|13C5)
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.12.180   Gi0/1         192.168.60.163  06 092A 13C4    26
Gi0/0         192.168.11.220   Gi0/1         192.168.60.20   06 0C09 13C5    11
Gi0/0         192.168.11.150   Gi0/1         192.168.60.245  06 0B66 09D5    18
Gi0/0         192.168.13.7     Gi0/1         192.168.60.162  06 0914 07D0    21
Gi0/0         192.168.41.86    Gi0/1         192.168.60.27   06 0B7B 06B8    32
router#
```

Cisco ASA、PIX、および FWSM ファイアウォール

緩和策： トランジット アクセス コントロール リスト

インターネット接続ポイント、パートナーおよびサプライヤー接続ポイントを含むかもしれない、入力アクセス ポイントでネットワークに入るネットワークまたは VPN 接続ポイントをトラフィックから保護するために、管理者はポリシー適用を行うために tACLs を展開するために助言されます。 tACL の構築は、既存のセキュリティ ポリシーと設定に基づいて、入力アクセス ポイントからネットワーク内に入ることを許可されたトラフィックのみを明示的に許可するか、ネットワークを通過することを許可されたトラフィックを許可することによって達成されます。 tACL 回避策はこれらの脆弱性に対して不正侵入が信頼されたソース ソース· アドレスから起きるとき完全な保護を提供できません。

tACL ポリシーは TCPポート 2000 年の不正 な SCCP パケットを、TCP ポート 5060 および 5061 影響を受けたデバイスに送信 されるおよび UDP ポート 5060 の TCP ポート 1720 および 2517 および SIP パケットの H.323 パケット拒否します。 次の例では、192.168.60.0/24 は影響を受けたデバイスによって使用する、192.168.100.1 のホストは影響を受けたデバイスへのアクセスを必要とする信頼されたソースとみなされます IP アドレス領域であり。 許可されないすべてのトラフィックを拒否する前に、ルーティングおよび管理アクセスに必要なトラフィックを許可するように注意する必要があります。

tACLs についての追加情報はアクセス コントロール リスト（ACL）送信中です: エッジでのフィルタリング』を参照してください。

```
! !-- Include explicit permit statements for trusted sources !-- that require access on the
vulnerable ports ! access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 2000 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq h323 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 2517 access-list tACL-Policy extended permit tcp
host 192.168.100.1 192.168.60.0 255.255.255.0 eq sip access-list tACL-Policy extended permit tcp
host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended permit
udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq sip ! !-- The following vulnerability-
specific access control entries !-- (ACEs) can aid in identification of attacks ! access-list
tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 2000 access-list tACL-Policy
extended deny tcp any 192.168.60.0 255.255.255.0 eq h323 access-list tACL-Policy extended deny
tcp any 192.168.60.0 255.255.255.0 eq 2517 access-list tACL-Policy extended deny tcp any
```

```
192.168.60.0 255.255.255.0 eq sip access-list tACL-Policy extended deny tcp any 192.168.60.0
255.255.255.0 eq 5061 access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0
eq sip ! !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations ! !-- Explicit deny for all other IP traffic !
access-list tACL-Policy extended deny ip any any ! !-- Apply tACL to interface(s) in the ingress
direction ! access-group tACL-Policy in interface outside
```

緩和策： Unicast Reverse Path Forwarding を使用したスプーフィング保護

この資料に説明があるいくつかの脆弱性はスプーフィングされたIP パケットによって不正利用することができます。 ユニキャスト RPF の適切な配備および設定は次の脆弱性に関するスプーフィングに保護 メカニズムを提供できます:

- UDP パケットを使用する SIP Denial of Service（DoS/DDoS）脆弱性

ユニキャスト RPF はインターフェイス レベルで設定され、検証可能な送信元 IP アドレスを持たないパケットを検出して廃棄できます。 管理者はユニキャスト RPF にスプーフィングされたパケットがソース IP アドレス 存在にユニキャストによって RPF 有効に されるインターフェイスを通してネットワークに適切な帰りルート入るかもしれないので完全なスプーフィング保護を提供するために頼るべきではありません。 エンタープライズ環境では、ユニキャスト RPF がインターネット エッジとレイヤ 3 インターフェイスの内部アクセス レイヤで有効になっている可能性があります。

ユニキャスト RPF の設定と使用についての詳細は、『Cisco セキュリティ アプライアンス コマンド リファレンス』の「ip verify reverse-path」と Applied Intelligence white paper『Unicast Reverse Path Forwarding について』を参照してください。

識別策： トランジット アクセス コントロール リスト

tACL がインターフェイスに加えられた後、管理者は TCP ポート 5060 および 506 ずっとフィルタ処理されたであるおよび UDP ポート 5060 の TCP ポート 1720 および 2517 および SIP パケットの H.323 パケット TCPポート 2000 年の SCCP パケットの数を確認する **show access-list コマンドを**使用できます。 管理者はこれらの脆弱性を不正利用する試みであるかどうか判別するためにフィルタ処理されたパケットを調査するために助言されます。 **show access-list tACL ポリシー**のための出力例は続きます:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 13 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0
eq 2000 (hitcnt=3)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0
eq h323 (hitcnt=24)
access-list tACL-Policy line 3 extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0
eq 2517 (hitcnt=20)
access-list tACL-Policy line 4 extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0
eq sip (hitcnt=14)
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0
eq 5061 (hitcnt=4)
access-list tACL-Policy line 6 extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0
eq sip (hitcnt=24)
access-list tACL-Policy line 7 extended deny tcp any 192.168.60.0 255.255.255.0 eq 2000 (
hitcnt=40)
access-list tACL-Policy line 8 extended deny tcp any 192.168.60.0 255.255.255.0 eq h323 (
hitcnt=31)
access-list tACL-Policy line 9 extended deny tcp any 192.168.60.0 255.255.255.0 eq 2517 (
```

```
hitcnt=29)
access-list tACL-Policy line 10 extended deny tcp any 192.168.60.0 255.255.255.0 eq sip (
hitcnt=13)
access-list tACL-Policy line 11 extended deny tcp any 192.168.60.0 255.255.255.0 eq 5061 (
hitcnt=19)
access-list tACL-Policy line 12 extended deny udp any 192.168.60.0 255.255.255.0 eq sip (
hitcnt=11)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=8)
firewall#
```

前の例では、アクセス リスト tACL *ポリシー*は信頼できないホストかネットワークから受信される次のパケットを廃棄しました:

- ACE ラインのための 7 **TCPポート 2000 年の 40 の SCCP** パケット
- ACE ラインのための 8 **TCPポート 1720 の H.323 31 の**パケット
- ACE ラインのための 9 **TCPポート 2517 の H.323 29 の**パケット
- ACE ラインのための 10 **TCPポート 5060 の 13 の SIP** パケット
- ACE ラインのための 11 **TCPポート 5061 の 19 の SIP** パケット
- ACE ラインのための 12 **UDP ポート 5060 の 11 の SIP** パケット

識別策： syslog

log キーワードを含まないアクセス コントロール エントリ（ACE）によって拒否されたパケットに対しては、ファイアウォール syslog メッセージ *106023* が生成されます。 この syslog メッセージについての追加情報は Ciscoセキュリティ アプライアンス システムログメッセージに-106023 あります。

Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス（ASA）ソフトウェア設定することについての情報はセキュリティ アプライアンスの監視にまたは Cisco PIX 500 シリーズ セキュリティ アプライアンスのための Syslog を-ログを設定・管理することあります。 Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのための FWSM の Syslog の設定についての情報は Firewall Services Module の監視にあります。

次の例では、**show logging | グレップ** *regex* コマンドはファイアウォールの口ギング バッファから syslog メッセージを得ます。 これらのメッセージはこの資料に説明がある脆弱性を不正利用する潜在的な試みを示す可能性がある拒否されたパケットについての追加情報を提供します。 **grep** キーワードを付けて別の正規表現を使用すると、ログ メッセージに含まれる特定のデータを検索できます。

正規表現構文についての追加情報は正規表現の作成にあります。

```
firewall#show logging | grep 106023
  Mar 24 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/2000 by access-group "tACL-Policy"
  Mar 24 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/1720 by access-group "tACL-Policy"
  Mar 24 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/2517 by access-group "tACL-Policy"
  Mar 24 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/5060 by access-group "tACL-Policy"
  Mar 24 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/5061 by access-group "tACL-Policy"
  Mar 24 2010 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.175/2950
         dst inside:192.168.60.250/5060 by access-group "tACL-Policy"
firewall#
```

ASA および PIX セキュリティ アプライアンスのための syslog メッセージについての追加情報は

Ciscoセキュリティ アプライアンス システムログメッセージにあります。 FWSM のための syslog メッセージについての追加情報はシステムログメッセージを記録 する Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ Firewall Services Module にあります。

syslog イベントを使用して調査事件についての追加情報に関しては、ファイアウォールおよび IOS ルータ Syslog イベントによって加えられる知性 白書を使用して識別事件を参照して下さい。

識別策： Unicast Reverse Path Forwarding を使用したスプーフィング保護

ユニキャスト RPF によって拒否されたパケットに対しては、ファイアウォール syslog メッセージ *106021* が生成されます。 この syslog メッセージについての追加情報は Ciscoセキュリティ アプライアンス システムログメッセージに- 106021 あります。

Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス (ASA) ソフトウェア設定することについての情報はセキュリティ アプライアンスの監視にまたは Cisco PIX 500 シリーズ セキュリティ アプライアンスのための Syslog を-ログを設定・管理することあります。 Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのための FWSM の Syslog の設定についての情報は Firewall Services Module の監視にあります。

次の例では、**show logging | グレップ** *regex* コマンドはファイアウォールの口ギング バッファから syslog メッセージを得ます。 これらのメッセージはこれらの脆弱性を不正利用する潜在的な試みを示す可能性がある拒否されたパケットについての追加情報を提供しますこの資料に説明がある。 **grep** キーワードを付けて別の正規表現を使用すると、ログ メッセージに含まれる特定のデータを検索できます。

正規表現構文についての追加情報は正規表現の作成にあります。

```
firewall#show logging | grep 106021
  Mar 24 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Mar 24 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Mar 24 2010 00:15:13: %ASA-1-106021: Deny TCP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
```

提示非対称多重処理システム drop コマンドはまた次の例に示すようにユニキャスト RPF 機能が廃棄したパケットの数を確認できます:

```
firewall#show asp drop frame rpf-violated
  Reverse-path verify failed                      11
firewall#
```

前記の例では、ユニキャスト RPF が設定されたインターフェイスで、受信した **11 個の IP パケット**が廃棄されています。 出力の不在はファイアウォールのユニキャスト RPF 機能がパケットを廃棄しなかったことを示します。

デバッグについての追加情報に関してはセキュリティ パスによって廃棄されたパケットを加速しましたまたは接続は、Ciscoセキュリティ アプライアンス コマンドレファレンスをのための**示します非対称多重処理システム ドロップするを**参照します。

Cisco Intrusion Prevention System

緩和策： Cisco IPS シグニチャ イベント アクション

管理者は脅威 検出を提供し、この資料に説明がある脆弱性を不正利用する試みを防ぐのを助けるのに Cisco 侵入防御システム（IPS）アプライアンスおよびサービス モジュールを使用できます。 これらの脆弱性は、次のシグニチャによって検出されることがあります。

- 24781/0 - Cisco IOS ソフトウェア 不正 な SCCP 脆弱性
- 24799/0 - Cisco IOS ソフトウェア 不正 な SCCP 脆弱性
- 24899-0 - Cisco IOS ソフトウェア H.323 DoS
- 24119/0 - Cisco CUBE SIP 脆弱性
- 24600/0 - Cisco IOS ソフトウェア SIP DoS
- 24760/0 - Cisco IOS ソフトウェア SIP DoS

24781/0 - Cisco IOS ソフトウェア 不正 な SCCP 脆弱性

Cisco IPS バージョン 6.x または 5.x を実行するセンサーのためのシグニチャアップデート S479 にはじまってこの脆弱性はシグニチャ 24781/0（シグニチャ名前によって検出することができます: Cisco IOS ソフトウェア 不正 な SCCP 脆弱性）。 シグニチャ 24781/0 は、誘発します*高い* severityイベントを、持ち 90 の（SFR）評価するシグニチャ 忠実度を生成**アラート**の既定のイベント操作で設定されますデフォルトで有効に なります。

シグニチャ 24799/0 は Cisco IOS ソフトウェアの不正 な SCCP 脆弱性を不正利用する試みを検出した上で起動 します。 このシグニチャの発生はこの脆弱性の潜在的なエクスプロイトを示すかもしれません。

24799/0 - Cisco IOS ソフトウェア 不正 な SCCP 脆弱性

Cisco IPS バージョン 6.x または 5.x を実行するセンサーのためのシグニチャアップデート S479 にはじまってこの脆弱性はシグニチャ 24799/0（シグニチャ名前によって検出することができます: Cisco IOS ソフトウェア 不正 な SCCP 脆弱性）。 シグニチャ 24799/0 は、誘発します*高い* severityイベントを、持ち 90 の（SFR）評価するシグニチャ 忠実度を生成**アラート**の既定のイベント操作で設定されますデフォルトで有効に なります。

シグニチャ 24799/0 は Cisco IOS ソフトウェアの不正 な SCCP 脆弱性を不正利用する試みを検出した上で起動 します。 このシグニチャの発生はこの脆弱性の潜在的なエクスプロイトを示すかもしれません。

24899-0 - Cisco IOS ソフトウェア H.323 DoS

Cisco IPS バージョン 6.x または 5.x を実行するセンサーのためのシグニチャアップデート S479 にはじまってこの脆弱性はシグニチャ 24899/0（シグニチャ名前によって検出することができます: Cisco IOS ソフトウェア H.323 DoS）。 シグニチャ 24899-0 は、誘発します*中間* severityイベントを、持ち 85 の（SFR）評価するシグニチャ 忠実度を生成**アラート**の既定のイベント操作で設定されますデフォルトで有効に なります。

シグニチャ 24899/0 は Cisco IOS ソフトウェアの H.323 DoS 脆弱性を不正利用する試みを検出した上で起動 します。 このシグニチャの発生はこの脆弱性の潜在的なエクスプロイトを示すかもしれません。

24119/0 - Cisco CUBE SIP 脆弱性

Cisco IPSversion 6.x か 5.x を経営するセンサーのためのシグニチャアップデート S479 にはじま

ってこの脆弱性はシグニチャ 24119/0 （シグニチャ名前によって検出することができます: Cisco CUBE SIP 脆弱性 ）。 シグニチャ 24119/0 は、誘発します*高い* severityイベントを、持ち 90 の signaturefidelity 定格（SFR ）を、生成**アラート**の既定のイベント操作で設定されますデフォルトで有効に なります。

シグニチャ 24119/0 は Cisco IOS ソフトウェアの CUBE SIP 脆弱性を不正利用する試みを検出した上で起動 します。 このシグニチャの発生はこの脆弱性の潜在的なエクスプロイトを示すかもしれません。

24600/0 - Cisco IOS ソフトウェア SIP DoS

Cisco IPS バージョン 6.x または 5.x を実行するセンサーのためのシグニチャアップデート S479 にはじまってこの脆弱性はシグニチャ 24600/0 （シグニチャ名前によって検出することができます: Cisco IOS ソフトウェア SIP DoS ）。 シグニチャ 24600/0 は、誘発します*中間* severityイベントを、持ち 85 の（SFR ）評価するシグニチャ 忠実度を生成**アラート**の既定のイベント操作で設定されますデフォルトで有効に なりません。

シグニチャ 24600/0 は Cisco IOS ソフトウェアの SIP DoS 脆弱性を不正利用する試みを検出した上で起動 します。 このシグニチャの発生はこの脆弱性の潜在的なエクスプロイトを示すかもしれません。

24760/0 - Cisco IOS ソフトウェア SIP DoS

Cisco IPS バージョン 6.x または 5.x を実行するセンサーのためのシグニチャアップデート S479 にはじまってこの脆弱性はシグニチャ 24760/0 （シグニチャ名前によって検出することができます: Cisco IOS ソフトウェア SIP DoS ）。 シグニチャ 24760/0 は、誘発します*中間* severityイベントを、持ち 80 の（SFR ）評価するシグニチャ 忠実度を生成**アラート**の既定のイベント操作で設定されますデフォルトで有効に なります。

シグニチャ 24760/0 は Cisco IOS ソフトウェアの SIP DoS 脆弱性を不正利用する試みを検出した上で起動 します。 このシグニチャの発生はこの脆弱性の潜在的なエクスプロイトを示すかもしれません。

管理者は攻撃が検出された際にイベント アクションを実行するように Cisco IPS センサーを設定できます。 設定された検知時のアクションはこの資料に説明がある脆弱性を不正利用するように試みている不正侵入から保護を助けるために予防か妨げる制御実行します。

スプーフィングされた IP アドレスを使用するエクスプロイトにより不注意に信頼されたソースからのトラフィックを拒否する設定された検知時のアクションを引き起こすかもしれません。

Cisco IPS センサーは、イベント アクションの使用と組み合せてインライン保護モードで配備すると、最も効果を発揮します。 インライン保護 モードで配備される Cisco IPS 6.x センサーのための自動脅威防止はこの資料に説明がある脆弱性を不正利用するように試みている不正侵入に対して脅威防止を提供します。 脅威防止は大きい *riskRatingValue* と誘発されたシグニチャのための検知時のアクションをより 90 行うデフォルト オーバーライドを通して実現します。

インライン保護 モードで配備される Cisco IPS 5.x センサーは毎シグニチャ基礎で設定される検知時のアクションを必要とします。 または、高リスクの脅威によってトリガーされたシグニチャに対してイベント アクションを実行できる上書き設定も可能です。 インライン保護 モードで配備されるセンサーの検知時のアクションを使用する最も有効なエクスプロイト防止を提供します。

計算を評価するリスク評価および脅威評価し、脅威評価参照リスクについての追加情報に関して

は: 簡素化する IPS ポリシー管理。

追加情報

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。

改訂履歴

リビジョン 1.1	2010 年 3 月 24 日	追加された IPS セクション。
リビジョン 1.0	2010 年 3 月 24 日	初版リリース

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html から入手できます。 この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。 すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

関連情報

- Cisco 適用対応策速報（英語）
- Ciscoセキュリティ情報収集活動
- Cisco IOS
- Cisco IOS NetFlow：Cisco.com のホーム ページ（英語）
- Cisco IOS NetFlow White Paper（英語）
- NetFlow パフォーマンス分析
- Cisco Network Foundation Protection White Paper（英語）
- Cisco Network Foundation Protection プレゼンテーション資料（英語）
- IP アドレッシングへのセキュリティ指向のアプローチ
- コントロール プレーン 保護の概要
- Tool Command Language on Cisco 保護します IOS を
- Cisco ファイアウォール製品：Cisco.com のホーム ページ（英語）
- Unicast Reverse Path Forwarding（uRPF）インターネット サービス プロバイダのための拡張
- Cisco 6.x 侵入防御システム（英語）
- Cisco IPS 6.x シグニチャ ダウンロード（英語）（登録ユーザ専用）
- Cisco IPS シグニチャ 検索ページ
- Cisco Security Monitoring, Analysis, and Response System
- Common Vulnerabilities and Exposures（CVE）