Cisco IOSソフトウェアの複数の機能におけるIPソケットの脆弱性

アドバイザリーID : cisco-sa-20090325-ip　CVE-2009-0630
初公開日 : 2009-03-25 00:00
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCsm27071

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

IPソケットの処理における脆弱性により、Cisco IOS?ソフトウェアが有効になっている。巧妙に細工された一連のTCP/IPパケットによって、次のような結果が生じる可能性があります。

- 設定された機能は、新しい接続またはセッションの受け入れを停止する可能性があります。
- デバイスのメモリが消費される可能性があります。
- デバイスのCPU使用率が長時間にわたって高くなることがあります。
- デバイスがリロードする可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。

このアドバイザリの「回避策」セクションでは、いくつかの緩和策について説明しています。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip で公開されています。

注：2009年3月25日のCisco IOSセキュリティアドバイザリバンドル公開には8件のSecurity Advisoryが含まれています。これらのアドバイザリはすべて、Cisco IOSソフトウェアの脆弱性に対処するものです。各アドバイザリには、そのアドバイザリに記載された脆弱性を修正するリリースが記載されています。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCPのDoS脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ctcp

- Cisco IOSソフトウェアの複数の機能におけるIPソケットの脆弱性 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip
- Cisco IOSソフトウェアモバイルIPおよびモバイルIPv6の脆弱性 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip
- Cisco IOSソフトウェアのSecure Copyにおける権限昇格の脆弱性 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp
- Cisco IOSソフトウェアのSession Initiation ProtocolにおけるDoS脆弱性 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip
- Cisco IOSソフトウェアの複数の機能における巧妙に細工されたTCPシーケンスの脆弱性 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp
- Cisco IOSソフトウェアの複数機能における巧妙に細工されたUDPパケットの脆弱性 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp
- Cisco IOSソフトウェアのWebVPNおよびSSLVPNの脆弱性 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

脆弱性のある製品

該当するバージョンのCisco IOSソフトウェアおよびCisco IOS XEソフトウェアを実行しているデバイスで次のいずれかの機能が実行されている場合、これらのデバイスが影響を受けます。影響を受ける機能がデバイスで有効になっているかどうかの確認の詳細については、このアドバイザリの「詳細」セクションを参照してください。

- Cisco Unified Communications Manager Express
- Transport Layer Security(TLS)トランスポートでのSIPゲートウェイシグナリングのサポート
- セキュアなシグナリングとメディア暗号化
- ブロック拡張交換プロトコル(BEEP)
- ネットワークアドミッションコントロールHTTP認証プロキシ
- EAPoUDP、Dot1x、およびMAC認証バイパスのためのユーザごとのURLリダイレクト
- HTTPリダイレクトを使用するDistributed Director
- DNS（TCPモードのみ）

シスコ製品で実行されているCisco IOSソフトウェアリリースは、管理者がデバイスにログイ

ンして、show versionコマンドを発行することにより確認できます。"Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。他のシスコデバイスには「show version」コマンドがないか、異なる出力が表示される場合があります。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
<#root>

Router#

show version

Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

次の例は、Cisco IOSソフトウェアリリース12.4(20)Tが稼働し、イメージ名がC1841-ADVENTERPRISEK9-Mである製品を示しています。

```
<#root>

Router#

show version

Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc3
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Cisco IOSソフトウェアリリースの命名規則の追加情報は、次のリンクの「White Paper: Cisco IOS Reference Guide」で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.html。

脆弱性を含んでいないことが確認された製品

次の製品は、この脆弱性の影響を受けません。

- Cisco IOS XR ソフトウェア
- Cisco 500シリーズワイヤレスExpressアクセスポイント
- Cisco Aironet 1250 シリーズ
- Cisco Aironet 1240 AG シリーズ
- Cisco Aironet 1230 AG シリーズ
- Cisco Aironet 1200 シリーズ
- Cisco Aironet 1140 シリーズ
- Cisco Aironet 1130 AG シリーズ
- Cisco Aironet 1100 シリーズ
- Cisco Aironet 1500 シリーズ
- Cisco Aironet 1400 シリーズ
- Cisco Aironet 1300 シリーズ
- Cisco AP801（860および880シリーズISR）
- Cisco WMIC(Cisco 3200 MAR)

Cisco IOSまたはCisco IOS XEソフトウェアで設定されたその他のシスコ製品や機能で、この脆弱性の影響を受けるものは現在確認されていません。

詳細

この脆弱性の不正利用を成功させるには、このセクションで説明されている機能のいずれかに対応するTCPポート番号に対して、TCP 3ウェイハンドシェイクを完了する必要があります。

Cisco Unified Communications Manager Express

次の設定は、異なるCisco Unified Communications Manager Expressサービスに対して脆弱です。

Certificate Authority Proxy Function(CAPF)サーバが設定されている。

次の例は、脆弱性のあるCAPFサーバ設定を示しています。

```
capf-server
 auth-mode null-string
 cert-enroll-trustpoint root password 1 104D000A061843595F
 trustpoint-label cme_cert
 source-addr 10.0.0.1
```

CAPFサーバに使用されるデフォルトのTCPポートは3804です。

CAPFサーバの詳細については、『Cisco Unified Communications Manager Express System Administrator Guide』

(http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeauth.html#wp108
照してください。

テレフォニーサービスのセキュリティパラメータが設定されている。

テレフォニーサービスのセキュリティパラメータが「device-security-mode」で設定されている場合、そのデバイスには脆弱性が存在します。次の例は、telephony-serviceセキュリティパラメータの脆弱性のある3つの設定を示しています。

```
ephone 1
 device-security-mode encrypted

ephone 2
 device-security-mode authenticated

ephone 3
 device-security-mode none
```

使用されるTCPポートは、テレフォニーサービス設定コマンドの「ip source-address <address> port <port-number>」で定義されます。

テレフォニーサービスのセキュリティパラメータの詳細については、『Cisco Unified Communications Manager Express System Administrator Guide』(http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeauth.html#wp108
照してください。

グローバルテレフォニーサービスまたはcall-manager-fallbackコマンドが設定されている。

グローバルな「telephony-service」または「call-manager-fallback」コマンドが設定されているCisco IOSコンフィギュレーションは、サブコマンドがtelephony-serviceまたはcall-manager-fallbackコンフィギュレーションモードである場合に脆弱です。次の例は、脆弱性のある設定を示しています。

```
telephony-service
 ip source-address 192.168.0.1 port 2011
```

または

```
call-manager-fallback
 ip source-address 192.168.0.1 port 2011
```

使用されるTCPポートは、「ip source-address <address> port <port-number>」設定コマンドで定義されます。

telephony serviceおよびcall-manager-fallbackの詳細については、『Cisco Unified Communications Manager Express System Administrator Guide』(http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmesystm.html)を参照してください。

TLSトランスポートでのSIPゲートウェイシグナリングサポート

注：SIPが有効なデバイスを使用しているお客様は、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sipでドキュメント『Cisco Security Advisory: Cisco IOS Session Initiation Protocol Denial of Service Vulnerability』も参照してください。

TLSトランスポートを介したSIPゲートウェイシグナリングサポートが設定されているデバイスには脆弱性が存在します。次の例は、脆弱性のある設定を示しています。

<#root>

```
voice service voip
 sip
  session transport tcp
```

tls

```
  url sips
```

--または--

<#root>

```
dial-peer voice 3456 voip
 voice-class sip url sips
 session protocol sipv2
 session transport tcp
```

tls

TLSトランスポートを介したSIPゲートウェイシグナリングのサポートが正しく機能するためには、管理者はまず次の設定を使用してトラストポイントを設定する必要があります。

```
sip-ua
     crypto signaling default trustpoint example_trustpoint_name
```

TLSトランスポート機能を介したSIPゲートウェイシグナリングサポートで使用されるデフォルトのTCPポートは5061です。

Cisco IOS SIPゲートウェイシグナリングのTLSトランスポート経由のサポートの詳細については、http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/FeatTLS.htmlにあるCisco IOSソフトウェアリリース12.4T機能ガイドを参照してください。

セキュアなシグナリングとメディア暗号化

デバイスは、DSPファーム会議機能のメディアおよびシグナリング暗号化(SRTP/TLS)、またはSkinny Call Control Protocol(SCCP)を使用するアナログ電話機のセキュアシグナリングおよびメディア暗号化で設定されている場合、脆弱性の影響を受けます。

次の例は、脆弱性のある3つの異なるセキュアDSPファーム設定を示しています。証明書やSCCP設定など、完全な設定には他の部分が必要ですが、これらの部分は簡略化のために除外されています。

```
<#root>

dspfarm profile 2 transcode

security

 trustpoint 2851ClientMina
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 codec g729r8
 codec g729br8
 maximum sessions 3
 associate application SCCP
```

```
<#root>

dspfarm profile 3 conference

security

 trustpoint sec2800-cfb
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 maximum sessions 2
 associate application SCCP
```

<#root>

```
dspfarm profile 5 mtp
```

security

```
 trustpoint 2851ClientMina
 codec g711alaw
 maximum sessions hardware 1
 associate application SCCP
```

DSPファーム会議上のメディアおよびシグナリング暗号化に使用されるデフォルトのTCPポートは2443です。

DSPファーム会議機能でのメディアおよびシグナリングの暗号化についての詳細は、次のリンクにある『Cisco IOSソフトウェアリリース12.4早期配布特別版』の http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/itsdsp.htmlを参照してください。

次の出力は、『アナログ電話機用のセキュアなシグナリングとメディア暗号化』の関連セクションを示しており、脆弱な設定です（証明書、SCCP設定、ダイヤルピアなど、完全な設定には他のいくつかの部分が必要です）。

<#root>

```
!--- The following lines show SCCP Telephony Control Application
!--- (STCAPP) security enabled at the system level:

stcapp ccm-group 1
```

stcapp security

```
 trustpoint analog
```

stcapp security mode

```
 encrypted
stcapp

<-- output removed for brevity -->

dial-peer voice 5002 pots
service stcapp

!--- The following line shows the security mode configured on the
!--- dial peer.
```

security mode

```
 authenticated
port 2/1
```

アナログ電話のメディアおよびシグナリング暗号化に使用されるデフォルトのTCPポートは2443です。

アナログ電話のメディアおよびシグナリング暗号化の詳細については、次のリンクの「Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide, Release 12.4T」を参照してください。
http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/fsxsecur.html。

Extensible Exchange Protocol(EXIP)のブロック

トランスポートプロトコルとしてBlocks Extensible Exchange Protocol(BEEP)を利用する設定コマンドまたは実行可能コマンドには、脆弱性が存在します。次の例は、NETCONF over BEEP機能の脆弱な設定を示しています。SASLを使用したNETCONF over BEEPにも脆弱性が存在します。

```
crypto key generate rsa general-keys
crypto pki trustpoint my_trustpoint
enrollment url http://10.2.3.3:80
subject-name CN=dns_name_of_host.com
revocation-check none

crypto pki authenticate my_trustpoint
crypto pki enroll my_trustpoint

line vty 0 15
netconf lock-time 60
netconf max-sessions 16

netconf beep initiator host1 23 user my_user password
   my_password encrypt my_trustpoint
reconnect-time 60

netconf beep listener 23 sasl user1 encrypt my_trustpoint
```

使用されるTCPポートは、「netconf beep initiator」および「netconf beep listener」設定コマンドで定義されます。

NETCONF over BEEPの詳細については、次のリンクにある『Cisco IOS Software Release 12.4T feature guide』http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htnetbe.html#wp1049404を参照してください。

BEEP実行コマンド「bingd」および「bingng」により、この脆弱性が呼び出されたときにトリガーされる可能性があります。次に、これらのコマンドの実行例を示します。

```
bingng device 192.168.0.1 23
bingd device 23
```

ネットワークアドミッションコントロールHTTP認証プロキシ

Network Admission Control（NAC；ネットワークアドミッションコントロール）HTTP認証プロキシが設定されているデバイスには脆弱性が存在します。デバイスが脆弱であるためには、認証プロキシルールが存在し、インターフェイスに適用されている必要があります。

次の設定では、認証プロキシルールを作成します。

```
ip admission name example-ap-rule-name proxy http
```

次の設定では、前の例で作成した認証プロキシルールをインターフェイスに適用しています。

```
interface GigabitEthernet 0/0
 ip admission example-ap-rule-name
```

ネットワークアドミッションコントロール(NAC)HTTP認証プロキシに使用されるデフォルトのTCPポートは80です。

Network Admission Control（NAC；ネットワークアドミッションコントロール）HTTP認証プロキシの詳細については、『Cisco IOS Security Configuration Guide, Release 12.4』(http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_net_admssn_ctrl_external_docbas
照してください。

EAPoUDP、Dot1x、およびMAC認証バイパスのためのユーザごとのURLリダイレクト

URLリダイレクト機能が設定されているデバイスには脆弱性が存在します。URLリダイレクトは、EAP over UDP(EAPoUDP)、Dot1x、およびMAC認証バイパス(MAB)認証メカニズムでサポートされています。URLリダイレクト設定は、サーバ上で行うことも、ローカルに定義されたプロファイルまたはポリシーの一部として設定することもできます。両方の設定に脆弱性が存在します。次のいずれかの設定のデバイスには脆弱性が存在します。

EAPoUDPに対するURLリダイレクト機能の有効化

URLリダイレクト機能は、次のグローバルコンフィギュレーションコマンドを使用してEAPoUDPに対して有効にします。

```
ip admission name <EAPoUDP-rule-name> eapoudp
```

次の設定では、前の例で作成したEAPoUDPルールをインターフェイスに適用します。

```
ip admission name <EAPoUDP-rule-name>
```

Dot1xおよびMABに対するURLリダイレクト機能の有効化

Dot1xとMABの両方のURLリダイレクト機能には脆弱性があり、次のような方法で定義されたRADIUSサーバ上にURLリダイレクトAVペアが存在します。

```
url-redirect="http://example.com"
url-redirect="urlacl"
```

Dot1xおよびMAB URLリダイレクト機能がスイッチで正常に動作するには、最低限、次の設定も必要です。URLリダイレクト用のインターフェイス固有の設定はありません。基本的に、インターフェイスはDot1x/MAB用に設定する必要があります。

```
ip http {server | secure-server}
ip device tracking
```

EAPoUDP、Dot1x、およびMABに対するユーザごとのURLリダイレクトに使用されるデフォルトのTCPポートは80および443です。

EAPoUDP、Dot1x、およびMABに対するユーザごとのURLリダイレクトの詳細については、『Catalyst 4500 Series Switch Software Configuration Guide, 12.2(50)SG』(http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/50sg/configuration/guide/dot1x.html#wp
照してください。

HTTPリダイレクトを使用するDistributed Director

Distributed DirectorがHTTPリダイレクトを使用して設定されている場合、デバイスに脆弱性が存在します。次の例は、脆弱性のある設定を示しています。

```
ip director ip-address 192.168.0.1
```

HTTPリダイレクトでDistributed Directorに使用されるデフォルトのTCPポートは53です。

HTTPリダイレクトを使用するDistributed Directorの詳細については、
http://www.cisco.com/en/US/products/hw/contnetw/ps813/products_tech_note09186a00801fa9dd.shtml#t
「Distributed Director Configuration Example Overview」を参照してください。

DNS

Cisco IOS DNS機能が設定されているデバイスには脆弱性が存在します。純粋なDNS over UDP実装には脆弱性はありません。デバイスへのDNS over TCPトラフィックのフィルタリングについては、このアドバイザリの「回避策」セクションを参照してください。次の例に示すコマンドのいずれかがデバイス設定に含まれている場合、そのデバイスには脆弱性が存在します。

```
ip dns server
ip dns primary example.com soa www.example.com admin@example.com
ip dns spoofing 192.168.0.1
```

DNSに使用されるデフォルトのTCPポートは53です。

Cisco IOS DNSの詳細については、次のリンクにある『Cisco IOS IP Addressing Services Configuration Guide, Release 12.4』を参照してください。
http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_config_dns_ps6350_TSD_Products_C

この脆弱性は、Cisco Bug ID CSCsm27071 (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-0630が割り当てられています。

回避策

この脆弱性に対する次の緩和策が確認されています。

インフラストラクチャ アクセス コントロール リスト

ネットワークを通過するトラフィックを遮断することはしばしば困難ですが、インフラストラクチャ デバイスをターゲットとした許可すべきではないトラフィックを特定し、そのようなトラフィックをネットワークの境界で遮断することは可能です。Infrastructure Access Control Lists (iACLs) は、ネットワークセキュリティのベストプラクティスであり、特定の脆弱性に対する回避策であると同時に長期に渡って役立つネットワークセキュリティを付加することができます。以下の iACL の例は、Infrastructure access-list の一部として設定されるべきであり、インフラストラクチャ IP アドレスの範囲に含まれる IP アドレスを持つ全ての機器を防御します:

```
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---
!--- Feature: Cisco Unified Communications Manager Express
!---
!--- CAPF server configuration
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 3804


!---
!--- Telephony-Service configuration
!--- The TCP port is as per the
ip source-address
!---
            port
 telephony
!--- service configuration command.  Example below 2999
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 2999


!---
!--- Deny Cisco Unified Communications Manager Express traffic
!--- from all other sources destined to infrastructure addresses.
!---


access-list 150 deny tcp any
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 3804
access-list 150 deny tcp any
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 2999


!---
!--- Feature: SIP Gateway Signaling Support Over TLS Transport
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 5061
```

```
!--- Deny SIP Gateway Signaling Support Over TLS Transport
!--- traffic from all other sources destined to infrastructure
!--- addresses.


access-list 150 deny tcp any
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 5061


!---
!--- Feature: Secure Signaling and Media Encryption
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 2443


!--- Deny Secure Signaling and Media Encryption traffic from all
!--- other sources destined to infrastructure addresses.


access-list 150 deny tcp any
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 2443


!---
!--- Feature: Blocks Extensible Exchange Protocol (BEEP)
!--- The TCP port used is defined with the

netconf beep initiator


!--- and

netconf beep listener

 configuration
!--- commands.  This example uses 3001
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 3001


!--- Deny BEEP traffic from all other sources destined to
!--- infrastructure addresses.


access-list 150 deny tcp any
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 3001


!---
!--- Feature: Network Admission Control HTTP Authentication Proxy
!--- and
!--- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 80
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 443


!---
!--- Deny Network Admission Control HTTP Authentication Proxy
!--- and
!--- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass traffic to infrastructue
!---


access-list 150 deny tcp any
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 80
access-list 150 deny tcp any
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 443


!---
!--- Features: Distributed Director with HTTP Redirects and DNS
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 53


!--- Deny Distributed Director with HTTP Redirects traffic and DNS
!--- from all other sources destined to infrastructure addresses.


access-list 150 deny tcp any
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 53


!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and configurations
!--- Permit all other traffic to transit the device.


access-list 150 permit ip any any


!--- Apply access-list to all interfaces (only one example shown)


interface serial 2/0
ip access-group 150 in
```

ホワイトペーパー『Protecting Your Core: Infrastructure Protection Access Control Lists』には、アクセスリストによるインフラストラクチャ保護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。このWhite Paperは、次のリンク先で入手できます。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

受信ACL(rACL)

分散型のプラットフォームにおいては、Cisco12000 シリーズ(GSR) では 12.0(21)S2、Cisco7500 シリーズでは 12.0(24)S、Cisco10720 シリーズでは 12.0(31)S の IOS ソフトウェアにてサポートされている Receive ACL も選択肢となります。受信 ACL は、ルート プロセッサが有害なトラフィックの影響を受ける前に、そのトラフィックからデバイスを保護します。受信 ACL は、それが設定されたデバイスのみを保護する設計になっています。Cisco 12000, 7500, 10720 では通過トラフィックは Receive ACL による影響を受けません。このため、以下の ACL の例において宛先 IP アドレス "any" が用いられても、自ルータの物理あるいは仮想 IP アドレスのみが参照されます。受信 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。ホワイトペーパー『GSR: Receive Access Control Lists』では、デバイスへの正当なトラフィックを識別して許可し、望ましくないパケットをすべて拒否することができます。このWhite Paperは、次のリンク先で入手できます。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml

次の receive path ACL は信頼できるホストからのこのようなタイプのトラフィックを許可するように記述されています。

<#root>

```
!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---

!---
!--- Feature: Cisco Unified Communications Manager Express
!---
!---

!---
!--- Permit CAPF server traffic from trusted hosts allowed to
!--- the RP.
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 3804


!---
!--- Telephony-Service configuration
!---

!---
!--- The TCP port is as per the

ip source-address

!---
```

port

```
 telephony-service
!--- configuration command.  Example below 2999
!---
!--- Permit Telephony-Service traffic from trusted hosts allowed
!--- to the RP.


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 2999


!---
!--- Deny Cisco Unified Communications Manager Express
!--- traffic from all other sources to the RP.
!---


access-list 150 deny tcp any any eq 3804
access-list 150 deny tcp any any eq 2999


!---
!--- Permit SIP Gateway Signaling Support Over TLS Transport
!--- traffic from trusted hosts allowed to the RP.
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 5061


!---
!--- Deny SIP Gateway Signaling Support Over TLS Transport
!--- traffic from all other sources to the RP.
!---



access-list 150 deny tcp any any eq 5061


!---
!--- Permit Secure Signaling and Media Encryption traffic
!--- from trusted hosts allowed to the RP.
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 2443


!---
!--- Deny Secure Signaling and Media Encryption traffic from
!--- all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 2443


!---
!--- Feature: Blocks Extensible Exchange Protocol (BEEP)
!--- The TCP port used is defined with the

netconf beep initiator


!--- and

netconf beep listener

 configuration commands.
!--- This example uses 3001
!---

!---
!--- Permit BEEP traffic from trusted hosts allowed to the RP.
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 3001


!---
!--- Deny BEEP traffic from all other sources to the RP.
!---


access-list 150 deny tcp any any eq 3001


!---
!--- Feature: Network Admission Control HTTP Authentication Proxy
!--- and
!--- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass
!---

!---
!--- Permit Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass traffic from trusted hosts allowed to
!--- the RP.
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 80
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 443


!---
!--- Deny Network Admission Control HTTP Authentication Proxy
!--- and
!--- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass traffic from all other sources to
!--- the RP.
!---
```

```
access-list 150 deny tcp any any eq 80
access-list 150 deny tcp any any eq 443


!---
!--- Features: Distributed Director with HTTP Redirects and DNS
!---

!---
!--- Permit Distribute Director and DNS traffic from trusted hosts
!--- allowed to the RP.
!---


access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 53


!---
!--- Deny distributed director and DNS traffic from all other
!--- sources to the RP.
!---


access-list 150 deny tcp any any eq 53


!---
!--- Permit all other traffic to the RP.
!--- according to security policy and configurations.
!---


access-list 150 permit ip any any


!---
!--- Apply this access list to the 'receive' path.
!---


ip receive access-list 150
```

コントロール プレーン ポリシング

Control Plane Policing(CoPP)を使用して、影響を受ける機能のデバイスへのTCPトラフィックアクセスをブロックできます。Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T は、CoPP 機能をサポートしています。管理およびコントロールプレーンを保護するために CoPP を機器に設定し、既存のセキュリティーポリシーとコンフィギュレーションに従って認定されたトラフィックだけがインフラストラクチャデバイス宛に送信されることを明示的に許可することで、インフラストラクチャへの直接攻撃のリスクとその効果を最小限に抑えることができます。下記の CoPP の例はインフラストラクチャ IP アドレスの範囲内にある IP アドレスを持つ全ての機器を保護するために定義される CoPP の一部として含まれるべき項目で

す：

<#root>

```
!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---
!--- Feature: Cisco Unified Communications Manager Express
!---
!--- CAPF Server configuration
!---


access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 3804


!---

!--- Telephony-Service configuration
!--- The TCP port is as per the
ip source-address
!---


 port



 telephony-service
!--- configuration command.  Example below 2999
!---


access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 2999


!---
!--- Permit Cisco Unified Communications Manager Express traffic
!--- sent to all IP addresses configured on all interfaces of
!--- the affected device so that it will be policed and dropped
!--- by the CoPP feature
!---
!--- CAPF server configuration
!---


access-list 150 permit tcp any any eq 3804


!---
!--- Telephony-Service configuration
!---
```

```
access-list 150 permit tcp any any eq 2999


!---
!--- Feature: SIP Gateway Signaling Support Over TLS Transport
!---


access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 5061


!---
!--- Permit SIP Gateway Signaling Support Over TLS Transport
!--- traffic sent to all IP addresses configured on all interfaces
!--- of the affected device so that it will be policed and
!--- dropped by the CoPP feature
!---


access-list 150 permit tcp any any eq 5061


!---
!--- Feature: Secure Signaling and Media Encryption
!---


access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 2443


!---
!--- Permit Secure Signaling and Media Encryption traffic sent to
!--- all IP addresses configured on all interfaces of the affected
!--- device so that it will be policed and dropped by the CoPP
!--- feature
!---


access-list 150 permit tcp any any eq 2443


!---
!--- Feature: Blocks Extensible Exchange Protocol (BEEP)
!--- The TCP port used is defined with the

netconf beep initiator


!--- and

netconf beep listener

 configuration commands.
!--- This example uses 3001
!---


access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 3001
```

```
!---
!--- Permit BEEP traffic sent to all IP addresses configured
!--- on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature
!---


access-list 150 permit tcp any any eq 3001


!---
!--- Feature: Network Admission Control HTTP Authentication Proxy
!--- and
!--- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass
!---


access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 80
access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 443


!---
!--- Permit Network Admission Control HTTP Authentication Proxy
!--- and Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature
!---


access-list 150 permit tcp any any eq 80
access-list 150 permit tcp any any eq 443


!---
!--- Features: Distributed Director with HTTP Redirects and DNS
!---


access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 53


!---
!--- Permit Distributed Director with HTTP Redirects and DNS
!--- traffic sent to all IP addresses configured on all interfaces
!--- of the affected device so that it will be policed and dropped
!--- by the CoPP feature
!---


access-list 150 permit tcp any any eq 53


!---
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
```

```
!--- to infrastructure devices
!---

!---
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
!---


class-map match-all drop-tcpip-class
match access-group 150


!---
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!---


policy-map drop-tcpip-traffic

class drop-tcpip-class
drop


!---
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
!---


control-plane
service-policy input drop-tcpip-traffic
```

上記の CoPP の例では、"permit" アクションであるアクセスコントロールリストエントリ (ACE) に該当し、攻撃である可能性のあるパケットは、policy-map の "drop" 機能により廃棄されますが、一方、"deny" アクション(記載されていません)に該当するパケットは、policy-map の "drop" 機能の影響を受けません。policy-map の構文は、12.2S と 12.0S Cisco IOS トレインでは異なるので注意が必要です:

```
policy-map drop-tcpip-traffic
class drop-tcpip-class
police 32000 1500 1500 conform-action drop exceed-action drop
```

CoPP機能の設定と使用についての詳細は、http://www.cisco.com/web/about/security/intelligence/coppwp_gs.htmlおよびhttp://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.htmlにある『Control Plane Policing Implementation Best Practices』および『Cisco IOS Software Releases 12.2 S - Control Plane Policing』を参照してください。

ネットワーク内のCiscoデバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Mitigation Bulletin』にて参照できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090325-tcp-and-ip

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	修正済みリリースの入手可能性	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	推奨リリース
12.0	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0DA	脆弱性あり(最初の修正は12.2DA)	12.4(18e) 12.4(23a)（2009年6月

		5日に入手可能）
12.0DB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0DC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0S	12.0(32)S12	12.0(32)S12
12.0SC	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0SL	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0SP	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0ST	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0SX	脆弱性あり(最初の修正は12.0S)	12.0(32)S12
12.0SY	12.0(32)SY8	12.0(32)SY8
12.0SZ	脆弱性あり(最初の修正	12.0(32)S12

	は12.0S)	
12.0T	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0W	脆弱性あり。TACに連絡	
12.0WC	脆弱性あり。TACに連絡	
12.0WT	脆弱性なし	
12.0XA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XE	脆弱性あり(最初の修正	12.4(18e)

	は12.4)	12.4(23a) (2009年6月5日に入手可能)
12.0XF	脆弱性なし	
12.0XG	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XI	12.0(4)XI2より前のリリースには脆弱性があり、12.0(4)XI2以降のリリースには脆弱性はありません。最初の修正は12.4です。	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XJ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XK	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.0XL	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)

12.0XM	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XN	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XQ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XR	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XS	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XT	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.0XV	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
Affected 12.1-Based	First Fixed Release（修正された最初のリリース）	推奨リリース

Releases		
12.1	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1AA	脆弱性あり。TACに連絡	
12.1AX	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.1AY	脆弱性あり(最初の修正は12.1EA)	12.1(22)EA13 12.2(44)SE6
12.1AZ	脆弱性あり(最初の修正は12.1EA)	12.1(22)EA13 12.2(44)SE6
12.1CX	脆弱性あり。TACに連絡	
12.1DA	脆弱性あり(最初の修正は12.2DA)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1DB	脆弱性あり。TACに連絡	
12.1DC	脆弱性あり。TACに連絡	

12.1E	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.1EA	12.1(22)EA13	12.1(22)EA13
12.1EB	脆弱性あり。TACに連絡	
12.1EC	脆弱性あり(最初の修正は12.3BC)	12.2(33)SCB1 12.3(23)BC6
12.1EO	脆弱性あり。TACに連絡	
12.1EU	脆弱性あり(最初の修正は12.2SG)	12.2(31)SGA9
12.1EV	脆弱性あり。TACに連絡	
12.1EW	脆弱性あり、 12.2SGAに移行	
12.1EX	脆弱性あり。TACに連絡	
12.1EY	脆弱性あり。TACに連絡	
12.1EZ	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16

12.1GA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1GB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1T	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月

		5日に入手可能）
12.1XF	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XG	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XI	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XJ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XL	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1XM	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）

12.1XP	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XQ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XR	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XS	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XT	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XU	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XV	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XW	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月

		5日に入手可能)
12.1XX	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XY	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1XZ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1YA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1YB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1YC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.1YD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)

12.1YE	12.1(5)YE6より前のリリースには脆弱性があり、12.1(5)YE6以降のリリースには脆弱性はありません。最初の修正は12.4です。	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YF	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.1YI	脆弱性あり。TACに連絡	
12.1YJ	脆弱性あり(最初の修正は12.1EA)	12.1(22)EA13 12.2(44)SE6
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）	推奨リリース
12.2	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2B	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月

		29日に入手可能）
12.2BC	脆弱性あり、 12.2SCB1または 12.3BCに移行	12.2(33)SCB1 12.3(23)BC6
12.2BW	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2BX	脆弱性あり、 12.2SB4に移行	12.2(33)SB4
12.2BY	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2BZ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2CX	脆弱性あり、 12.2SCBまたは 12.3BCに移行	12.2(33)SCB1 12.3(23)BC6
12.2CY	脆弱性あり、 12.2SCBまたは 12.3BCに移行	12.2(33)SCB1 12.3(23)BC6
12.2CZ	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4

12.2DA	12.2(12)DA14（2009年7月30日に入手可能）	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2DD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2DX	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2EW	脆弱性あり(最初の修正は12.2SG)	12.2(31)SGA9
12.2EWA	脆弱性あり(最初の修正は12.2SG)	12.2(31)SGA9
12.2EX	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2EY	12.2(44)EY	12.2(44)SE6
12.2EZ	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2FX	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2FY	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6

12.2FZ	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2IRA	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SRC4（2009年5月18日に入手可能）
12.2IRB	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SRC4（2009年5月18日に入手可能）
12.2IXA	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXB	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXC	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXD	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXE	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXF	脆弱性あり。12.2IXHの任意のリリースに移行	12.2(18)IXH（2009年3月31日に入手可能）
12.2IXG	脆弱性あり。	12.2(18)IXH（2009年

	12.2IXHの任意のリリースに移行	3月31日に入手可能）
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2MB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2MC	12.2(15)MC2m	12.2(15)MC2m
12.2S	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2SB	12.2(31)SB14 12.2(33)SB1 12.2(28)SB13	12.2(33)SB4
12.2SBC	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2SCA	12.2(33)SCA2	12.2(33)SCB1
12.2SCB	脆弱性なし	
12.2SE	12.2(50)SE	12.2(44)SE6

	12.2(46)SE2 12.2(44)SE5	
12.2SEA	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEB	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEC	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SED	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEE	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEF	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SEG	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE6
12.2SG	12.2(50)SG	12.2(52)SG（2009年5月15日に入手可能）
12.2SGA	12.2(31)SGA9	12.2(31)SGA9
12.2SL	脆弱性なし	
12.2SM	脆弱性あり。TACに連	

	絡	
12.2SO	脆弱性あり。TACに連絡	
12.2SQ	脆弱性なし	
12.2SRA	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SRC4（2009年5月18日に入手可能）
12.2SRB	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SRB5a（2009年4月3日に入手可能） 12.2(33)SRC4（2009年5月18日に入手可能）
12.2SRC	12.2(33)SRC1	12.2(33)SRC4（2009年5月18日に入手可能）
12.2SRD	脆弱性なし	
12.2STE	脆弱性あり。TACに連絡	
12.2SU	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2SV	脆弱性あり。TACに連絡	
12.2SVA	脆弱性あり。TACに連絡	

12.2SVC	脆弱性あり。TACに連絡	
12.2SVD	脆弱性あり。TACに連絡	
12.2SVE	脆弱性あり。TACに連絡	
12.2SW	脆弱性あり。TACに連絡	
12.2SX	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXA	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXB	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXD	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXE	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2SXF	12.2(18)SXF16	12.2(18)SXF16
12.2SXH	12.2(33)SXH5（2009年4月20日に入手可能）	12.2(33)SXH5（2009年4月20日に入手可能）
12.2SXI	脆弱性なし	

12.2SY	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2SZ	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.2T	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2TPC	脆弱性あり。TACに連絡	
12.2XA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XB	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XC	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XD	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月

		5日に入手可能）
12.2XF	脆弱性あり、 12.2SCBまたは 12.3BCに移行	12.2(33)SCB1 12.3(23)BC6
12.2XG	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XI	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XJ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XK	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XL	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2XM	脆弱性あり(最初の修正	12.4(18e)

	は12.4)	12.4(23a) (2009年6月5日に入手可能)
12.2XN	脆弱性あり(最初の修正は12.2SRC)	12.2(33)SB4 12.2(33)SRD1
12.2XNA	脆弱性あり。12.2SRDの任意のリリースに移行	12.2(33)SRD1
12.2XNB	脆弱性なし	
12.2XNC	脆弱性なし	
12.2XO	12.2(46)XO	12.2(46)XO
12.2XQ	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.2XR	脆弱性なし	
12.2XS	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.2XT	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.2XU	脆弱性あり(最初の修正	12.4(18e)

	は12.4)	12.4(23a) (2009年6月5日に入手可能)
12.2XV	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.2XW	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.2YA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a) (2009年6月5日に入手可能)
12.2YB	脆弱性あり。TACに連絡	
12.2YC	脆弱性あり。TACに連絡	
12.2YD	脆弱性あり。TACに連絡	
12.2YE	脆弱性あり。TACに連絡	
12.2YF	脆弱性あり。TACに連絡	
12.2YG	脆弱性あり。TACに連絡	

12.2YH	脆弱性あり。TACに連絡	
12.2YJ	脆弱性あり。TACに連絡	
12.2YK	脆弱性あり。TACに連絡	
12.2YL	脆弱性あり。TACに連絡	
12.2YM	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2YN	脆弱性あり。TACに連絡	
12.2YO	脆弱性あり。TACに連絡	
12.2YP	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2YQ	脆弱性あり。TACに連絡	
12.2YR	脆弱性あり。TACに連絡	

12.2YS	脆弱性なし	
12.2YT	脆弱性あり。TACに連絡	
12.2YU	脆弱性あり。TACに連絡	
12.2YV	脆弱性あり。TACに連絡	
12.2YW	脆弱性あり。TACに連絡	
12.2YX	脆弱性あり。TACに連絡	
12.2YY	脆弱性あり。TACに連絡	
12.2YZ	脆弱性あり。TACに連絡	
12.2ZA	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF16
12.2ZB	脆弱性あり。TACに連絡	
12.2ZC	脆弱性あり。TACに連絡	
12.2ZD	脆弱性あり。TACに連	

	絡	
12.2ZE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2ZF	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2ZG	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.2ZH	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.2ZJ	脆弱性あり。TACに連絡	
12.2ZL	脆弱性あり。TACに連絡	
12.2ZP	脆弱性あり。TACに連絡	
12.2ZU	脆弱性あり(最初の修正は12.2SXH)	12.2(33)SXH5（2009年4月20日に入手可能）
12.2ZX	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4

12.2ZY	脆弱性あり。TACに連絡	
12.2ZYA	12.2(18)ZYA1	12.2(18)ZYA1
Affected 12.3-Based Releases	First Fixed Release（修正された最初のリリース）	推奨リリース
12.3	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.3B	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3BC	12.3(23)BC6	12.3(23)BC6
12.3BW	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3EU	脆弱性なし	
12.3JA	脆弱性なし	
12.3JEA	脆弱性なし	
12.3JEB	脆弱性なし	

12.3JEC	脆弱性なし	
12.3JK	脆弱性なし	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3JL	脆弱性あり(最初の修正は12.4JK)	
12.3JX	脆弱性なし	
12.3T	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3TPC	脆弱性あり。TACに連絡	
12.3VA	脆弱性あり。TACに連絡	
12.3XA	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.3XB	脆弱性あり。TACに連絡	
12.3XC	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）

12.3XD	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XE	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.3XF	脆弱性あり。TACに連絡	
12.3XG	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XI	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB4
12.3XJ	脆弱性あり(最初の修正は12.3YX)	12.3(14)YX14
12.3XK	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XL	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XQ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月

		29日に入手可能）
12.3XR	脆弱性あり(最初の修正は12.4)	12.4(18e) 12.4(23a)（2009年6月5日に入手可能）
12.3XS	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XU	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XW	脆弱性あり(最初の修正は12.3YX)	12.3(14)YX14
12.3XX	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XY	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3XZ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YA	脆弱性あり(最初の修正は12.4T)	12.4(22)T1

		12.4(15)T9（2009年4月29日に入手可能）
12.3YD	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YF	脆弱性あり(最初の修正は12.3YX)	12.3(14)YX14
12.3YG	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YH	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YI	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YJ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YK	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YM	12.3(14)YM13	12.3(14)YM13

12.3YQ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YS	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YT	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YU	脆弱性あり(最初の修正は12.4XB)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.3YX	12.3(14)YX14	12.3(14)YX14
12.3YZ	脆弱性あり。TACに連絡	
12.3ZA	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	推奨リリース
12.4	12.4(19)	12.4(18e)

	12.4(18a) 12.4(23a)（2009年6月5日に入手可能）	12.4(23a)（2009年6月5日に入手可能）
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性あり。TACに連絡	
12.4JMB	脆弱性あり。TACに連絡	
12.4JX	脆弱性なし	
12.4MD	12.4(11)MD7	12.4(11)MD7
12.4MR	12.4(19)MR	12.4(19)MR2
12.4SW	脆弱性あり。TACに連絡	
12.4T	12.4(20)T 12.4(15)T8 12.4(15)T9（2009年4月29日に入手可能）	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）

12.4XA	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XB	12.4(15)T8 12.4(20)T	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XC	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XD	12.4(4)XD12（2009年3月27日に入手可能）	12.4(4)XD12（2009年3月27日に入手可能）
12.4XE	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XF	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XG	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XJ	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）

12.4XK	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XL	12.4(15)XL4	12.4(15)XL4
12.4XM	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XN	脆弱性あり。TACに連絡	
12.4XP	脆弱性あり。TACに連絡	
12.4XQ	12.4(15)XQ2	12.4(15)XQ2
12.4XR	12.4(15)XR4	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XT	脆弱性あり(最初の修正は12.4T)	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XV	脆弱性あり。TACに連絡	
12.4XW	12.4(11)XW10	12.4(11)XW10

12.4XY	12.4(15)XY4	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
12.4XZ	脆弱性なし	
12.4YA	脆弱性なし	
12.4YB	脆弱性なし	
12.4YD	脆弱性なし	

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、シスコ内部での脆弱性テストによって発見されたものです。また、この脆弱性を報告していただいたフリーランスコンサルタントのJens Link氏にも感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

改訂履歴

リビジョン 1.4	2009年6月25日	2009年3月9日の統合修正済みソフトウェアテーブルへの参照を削除。
リビジ	2009年	リリース12.4(23a)の公開予定日を更

ョン 1.3	6月1日	新。
リビジョン 1.2	2009年 5月1日	リリース12.4(23a)の公開予定日を更新。
リビジョン 1.1	2009年 3月30日	特に「Wireless Products as not affected（ワイヤレス製品は影響を受けない）」と表記
リビジョン 1.0	2009年 3月25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。