Cisco 10000、uBR10012、uBR7200シリーズデバイスのIPC脆弱性

アドバイザリーID : cisco-sa-20080924-ipc
初公開日 : 2008-09-24 16:00
バージョン 1.1 : Final
CVSSスコア : 8.5
回避策 : No Workarounds available
Cisco バグ ID : CSCsg15342 CSCsh29217

CVE-2008-3805
CVE-2008-3806

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

Cisco 10000、uBR10012、およびuBR7200シリーズのデバイスは、外部から到達可能なユーザデータグラムプロトコル(UDP)ベースのプロセス間通信(IPC)チャネルを使用します。攻撃者は、この脆弱性を不正利用して該当デバイスにサービス拒否(DoS)状態を引き起こす可能性があります。他のプラットフォームは影響を受けません。

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。この脆弱性に対しては回避策があります。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc で公開されています。

注：2008年9月24日のIOSアドバイザリバンドル公開には12件のSecurity Advisoryが含まれています。11件のアドバイザリはCisco IOSソフトウェアの脆弱性に対処するもので、1件はCisco Unified Communications Managerの脆弱性に対処するものです。各アドバイザリには、このアドバイザリで説明されている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。

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosips
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

20080924-cucm

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sccp
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosfw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-l2tp

該当製品

該当するバージョンのCisco IOSを実行しているCisco 10000、uBR10012、およびuBR7200シリーズデバイスが該当します。

脆弱性のある製品

Cisco IOSを実行しているデバイスは、show versionコマンドを使用して確認できます。次の例は、Cisco IOSソフトウェアリリース12.2(31)SB10eを実行しているCisco 10000シリーズデバイスからの出力を示しています。

<#root>

```
c10k#
show version | include IOS
Cisco IOS Software, 10000 Software (C10K3-P11-M), Version 12.2(31)SB10e, RELEASE SOFTWARE (fc1)
c10k#
```

次の例は、Cisco IOSソフトウェアリリース12.3(17b)BC7を実行しているCisco uBR10012シリーズデバイスからの出力を示しています。

<#root>

```
ubr10k#
show version | include IOS
```

```
IOS (tm) 10000 Software (UBR10K-K8P6U2-M), Version 12.3(17b)BC7, RELEASE SOFTWARE (fc1)
ubr10k#
```

次の例は、Cisco IOSソフトウェアリリース12.3(21a)BC2を実行しているCisco uBR7200シリーズデバイスからの出力を示しています。

```
<#root>

ubr7200#

show version | include IOS

IOS (tm) 7200 Software (UBR7200-IK9SU2-M), Version 12.3(21a)BC2, RELEASE SOFTWARE (fc1)
ubr7200#
```

Cisco IOSリリースの命名規則の詳細については、『White Paper: Cisco IOS Reference Guide』というドキュメントを参照してください。このドキュメントは、次のリンク先で確認できます。http://www.cisco.com/warp/public/620/1.html

下記の「ソフトウェアバージョンおよび修正」セクションに記載されている修正済みバージョンより前のCisco IOSのバージョンには、脆弱性が存在します。

脆弱性を含んでいないことが確認された製品

Cisco uBR7100シリーズデバイスは該当しません。

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

Cisco 10000、uBR10012、およびuBR7200シリーズのデバイスは、UDPベースのIPCチャネルを使用します。このチャネルは、127.0.0.0/8の範囲とUDPポート1975からのアドレスを使用します。該当するバージョンのCisco IOSを実行しているCisco 10000、uBR10012、およびuBR7200シリーズデバイスでは、デバイスの外部からUDPポート1975に送信されるIPCメッセージが処理されます。この動作は、攻撃者によってデバイス、ラインカード、またはその両方のリロードが引き起こされ、DoS状態が発生する可能性があります。

127.0.0.0/8またはUDPポート1975宛ての不正なトラフィックをフィルタリングすることで、この脆弱性を軽減できます。

この脆弱性は、Cisco Bug ID CSCsg15342（登録ユーザ専用）およびCSCsh29217(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-2008-3805が割り当てられています。

回避策

回避策は、127.0.0.0/8の範囲に送信されるパケットのフィルタリングと、ポート1975に送信されるUDPパケットで構成されます。

インターフェイスアクセスコントロールリストの使用

ポート1975宛てのUDPパケットをフィルタリングするアクセスリストを使用すると、この脆弱性を緩和できます。UDPポート1975は、特定のアプリケーションで使用できる登録済みのポート番号です。ただし、UDPポート1975宛てのすべてのパケットをフィルタリングすると、一部のアプリケーションが誤動作する可能性があります。したがって、アクセスリストは、任意のルータインターフェイスのIPアドレスに送信されるUDP 1975パケットを明示的に拒否し、通過トラフィックを許可する必要があります。このようなアクセスリストを有効にするには、すべてのインターフェイスに適用する必要があります。IPCチャネルは127.0.0.0/8の範囲のアドレスを使用するため、この範囲を送信元または宛先とするパケットをフィルタリングする必要もあります。次に例を示します。

```
access-list 100 deny udp any host <router-interface 1> eq 1975
access-list 100 deny udp any host <router-interface 2> eq 1975
access-list 100 deny udp any host <router-interface ...> eq 1975
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip any 127.0.0.0 0.255.255.255
access-list 100 permit ip any any

interface Serial 0/0
  ip access-group 100 in
```

コントロールプレーンポリシングの使用

コントロールプレーンポリシング(CoPP)を使用すると、信頼できないUDPポート1975から該当デバイスへのアクセスをブロックできます。CoPP機能は、Cisco IOSソフトウェアリリース12.2BCおよび12.2SCAでサポートされています。デバイスに CoPP を設定して、管理プレーンとコントロール プレーンを保護し、既存のセキュリティ ポリシーおよび設定に従って、インフラストラクチャのデバイスに送信される承認されたトラフィックだけ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効果を最小限に抑えることができます。次の例をネットワークに適用できます。

注：CoPPはuBR10012シリーズデバイスではサポートされていません。

```
!-- Permit all UDP/1975 traffic so that it
!-- will be policed and dropped by the CoPP feature
```

```
!
access-list 111 permit udp any any eq 1975
access-list 111 permit ip any 127.0.0.0 0.255.255.255
access-list 111 permit ip 127.0.0.0 0.255.255.255 any
!

!-- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and
!-- Layer 4 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-IPC-class
  match access-group 111
!

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

!
policy-map drop-IPC-traffic
  class drop-IPC-class
    drop
!

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

!
control-plane
  service-policy input drop-IPC-traffic
!
```

上記のCoPPの例では、access control list entries（ACE；アクセスコントロールリストエントリ）の潜在的な悪用パケットに「permit」アクションが一致する場合、これらのパケットはポリシーマップの「drop」機能によって廃棄されますが、「deny」アクション（非表示）に一致するパケットは、ポリシーマップのdrop機能の影響を受けません。

Cisco IOS 12.2Sトレインと12.0Sトレインでは、ポリシーマップの構文が異なることに注意してください。

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

CoPP機能の設定と使用方法の詳細については、

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html、
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd8
およびhttp://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.htmlを参照してください。

ネットワーク境界でのインフラストラクチャACLの使用

ネットワークを通過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決して許可すべきでは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。iACL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、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、またこの特定の脆弱性の回避策として考慮する必要があります。以下に示すiACL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アドレスを持つすべてのデバイスを保護するために配備されるインフラストラクチャアクセスリストの一部として含める必要があります。

```
!-- Note: IPC packets sent to UDP destination port 1975 must not
!--       be permitted from any trusted source as this traffic
!--       should only be sent and received internally by the
!--       affected device using an IP address allocated from the
!--       127.0.0.0/8 prefix.
!--
!--       IPC that traffic that is internally generated and sent
!--       and/or received by the affected device is not subjected
!--       to packet filtering by the applied iACL policy.

!

!-- Deny IPC (UDP port 1975) packets from all sources destined to
!-- all IP addresses configured on the affected device.

!
access-list 150 deny udp any host INTERFACE_ADDRESS#1 eq 1975
access-list 150 deny udp any host INTERFACE_ADDRESS#2 eq 1975
access-list 150 deny udp any host INTERFACE_ADDRESS#N eq 1975
!

!-- Deny all IP packets with a source or destination IP address
!-- from the 127.0.0.0/8 prefix.

!
access-list 150 deny ip 127.0.0.0 0.255.255.255 any
access-list 150 deny ip any 127.0.0.0 0.255.255.255
!


!-- 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 iACL to interfaces in the ingress direction.

!
interface GigabitEthernet0/0
  ip access-group 150 in
!
```

注：ポート1975宛てのUDPパケットをフィルタリングするiACLを使用すると、この脆弱性を緩和できます。ただし、UDPポート1975は、特定のアプリケーションで使用できる登録済みのポート番号です。UDPポート1975宛てのすべてのパケットをフィルタリングすると、一部のアプリケーションが誤動作する可能性があります。したがって、iACLポリシーでは、1975の宛先ポートを使用して、影響を受けるデバイスの任意のルータインターフェイスIPアドレスに送信されるUDPパケットを明示的に拒否し、既存のセキュリティポリシーと設定に従って他のすべてのレイヤ3およびレイヤ4トラフィックを許可または拒否し、他のすべてのトラフィックがデバイスを通過することを許可する必要があります。IPCチャネルは127.0.0.0/8の範囲のアドレスを使用するため、この範囲を送信元または宛先とするパケットも、前の例に示すようにフィルタリングする必要があります。

ホワイトペーパー『Protecting Your Core: Infrastructure Protection Access Control Lists』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 は次のサイトで提供されています。

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

その他の緩和策

ネットワーク内のCiscoデバイスに配備できる追加の緩和テクニックについては、このアドバイザリに関連するCisco適用対応策速報を参照してください。次のリンクから入手できます。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080924-ipc-and-ubr

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	脆弱性なし	
12.0DA	脆弱性なし	
12.0DB	脆弱性なし	
12.0DC	脆弱性なし	
12.0S	12.0(32)Sより前のリリースには脆弱性があり、12.0(32)S以降のリリースには脆弱性はありません。	12.0(32)S11 12.0(33)S1
12.0SC	脆弱性なし	
12.0SL	脆弱性あり、	

	12.0S、12.1に移行	
12.0SP	脆弱性なし	
12.0ST	脆弱性あり、 12.0S、12.1に移行	
12.0SX	脆弱性なし	
12.0SY	脆弱性なし	
12.0SZ	12.0(30)SZ4	12.0(32)S11 12.0(33)S1
12.0T	脆弱性なし	
12.0W	脆弱性なし	
12.0WC	脆弱性なし	
12.0WT	脆弱性なし	
12.0XA	脆弱性なし	
12.0XB	脆弱性なし	
12.0XC	脆弱性なし	
12.0XD	脆弱性なし	

12.0XE	脆弱性なし	
12.0XF	脆弱性なし	
12.0XG	脆弱性なし	
12.0XH	脆弱性なし	
12.0XI	脆弱性なし	
12.0XJ	脆弱性なし	
12.0XK	脆弱性なし	
12.0XL	脆弱性なし	
12.0XM	脆弱性なし	
12.0XN	脆弱性なし	
12.0XQ	脆弱性なし	
12.0XR	脆弱性なし	
12.0XS	脆弱性なし	
12.0XT	脆弱性なし	
12.0XV	脆弱性なし	

Affected 12.1-Based Releases	First Fixed Release（修正された最初のリリース）	推奨リリース
該当する 12.1 ベースのリリースはありません。		
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	脆弱性なし	
12.2B	脆弱性なし	
12.2BC	脆弱性なし	
12.2BW	脆弱性なし	
12.2BX	脆弱性なし	
12.2BY	脆弱性なし	
12.2BZ	脆弱性なし	
12.2CX	脆弱性なし	
12.2CY	脆弱性なし	
12.2CZ	脆弱性なし	

12.2DA	脆弱性なし	
12.2DD	脆弱性なし	
12.2DX	脆弱性なし	
12.2EW	脆弱性なし	
12.2EWA	脆弱性なし	
12.2EX	脆弱性なし	
12.2EY	脆弱性なし	
12.2EZ	脆弱性なし	
12.2FX	脆弱性なし	
12.2FY	脆弱性なし	
12.2FZ	脆弱性なし	
12.2IRB	脆弱性なし	
12.2IXA	脆弱性なし	
12.2IXB	脆弱性なし	
12.2IXC	脆弱性なし	

12.2IXD	脆弱性なし	
12.2IXE	脆弱性なし	
12.2IXF	脆弱性なし	
12.2IXG	脆弱性なし	
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性なし	
12.2MC	脆弱性なし	
12.2S	脆弱性なし	
12.2SB	12.2(31)SB13 12.2(33)SB1	12.2(33)SB2（2008年9月26日に入手可能）
12.2SBC	脆弱性なし	
12.2SCA	12.2(33)SCA1	12.2(33)SCA1
12.2SE	脆弱性なし	
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	

12.2SEC	脆弱性なし	
12.2SED	脆弱性なし	
12.2SEE	脆弱性なし	
12.2SEF	脆弱性なし	
12.2SEG	脆弱性なし	
12.2SG	脆弱性なし	
12.2SGA	脆弱性なし	
12.2SL	脆弱性なし	
12.2SM	脆弱性なし	
12.2SO	脆弱性なし	
12.2SRA	脆弱性なし	
12.2SRB	脆弱性なし	
12.2SRC	12.2(33)SRC2	12.2(33)SRC2
12.2SU	脆弱性なし	
12.2SV	脆弱性なし	

12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	
12.2SVD	脆弱性なし	
12.2SW	脆弱性なし	
12.2SX	脆弱性なし	
12.2SXA	脆弱性なし	
12.2SXB	脆弱性なし	
12.2SXD	脆弱性なし	
12.2SXE	脆弱性なし	
12.2SXF	脆弱性なし	
12.2SXH	脆弱性なし	
12.2SY	脆弱性なし	
12.2SZ	脆弱性なし	
12.2T	脆弱性なし	
12.2TPC	脆弱性なし	

12.2XA	脆弱性なし	
12.2XB	脆弱性なし	
12.2XC	脆弱性なし	
12.2XD	脆弱性なし	
12.2XE	脆弱性なし	
12.2XF	脆弱性なし	
12.2XG	脆弱性なし	
12.2XH	脆弱性なし	
12.2XI	脆弱性なし	
12.2XJ	脆弱性なし	
12.2XK	脆弱性なし	
12.2XL	脆弱性なし	
12.2XM	脆弱性なし	
12.2XN	脆弱性なし	
12.2XNA	脆弱性なし	

12.2XNB	脆弱性なし	
12.2XO	脆弱性なし	
12.2XQ	脆弱性なし	
12.2XR	脆弱性なし	
12.2XS	脆弱性なし	
12.2XT	脆弱性なし	
12.2XU	脆弱性なし	
12.2XV	脆弱性なし	
12.2XW	脆弱性なし	
12.2YA	脆弱性なし	
12.2YB	脆弱性なし	
12.2YC	脆弱性なし	
12.2YD	脆弱性なし	
12.2YE	脆弱性なし	
12.2YF	脆弱性なし	

12.2YG	脆弱性なし	
12.2YH	脆弱性なし	
12.2YJ	脆弱性なし	
12.2YK	脆弱性なし	
12.2YL	脆弱性なし	
12.2YM	脆弱性なし	
12.2YN	脆弱性なし	
12.2YO	脆弱性なし	
12.2YP	脆弱性なし	
12.2YQ	脆弱性なし	
12.2YR	脆弱性なし	
12.2YS	脆弱性なし	
12.2YT	脆弱性なし	
12.2YU	脆弱性なし	
12.2YV	脆弱性なし	

12.2YW	脆弱性なし	
12.2YX	脆弱性なし	
12.2YY	脆弱性なし	
12.2YZ	脆弱性なし	
12.2ZA	脆弱性なし	
12.2ZB	脆弱性なし	
12.2ZC	脆弱性なし	
12.2ZD	脆弱性なし	
12.2ZE	脆弱性なし	
12.2ZF	脆弱性なし	
12.2ZG	脆弱性なし	
12.2ZH	脆弱性なし	
12.2ZJ	脆弱性なし	
12.2ZL	脆弱性なし	
12.2ZP	脆弱性なし	

12.2ZU	脆弱性なし	
12.2ZX	脆弱性あり(最初の修正は12.2SB)	12.2(33)SB2（2008年9月26日に入手可能）
12.2ZY	脆弱性なし	
12.2ZYA	脆弱性なし	
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	脆弱性なし	
12.3B	脆弱性なし	
12.3BC	12.3(17b)BC6 12.3(21a)BC1 12.3(23)BC	12.3(23)BC4
12.3BW	脆弱性なし	
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	
12.3JL	脆弱性なし	
12.3JX	脆弱性なし	
12.3T	注：12.3(14)T3より前のリリースには脆弱性があり、12.3(14)T3以降のリリースには脆弱性はありません。	12.4(15)T7 12.4(18c)
12.3TPC	脆弱性なし	
12.3VA	脆弱性なし	
12.3XA	脆弱性なし	
12.3XB	脆弱性なし	
12.3XC	脆弱性なし	
12.3XD	脆弱性なし	
12.3XE	脆弱性なし	
12.3XF	脆弱性なし	

12.3XG	脆弱性なし	
12.3XI	12.3(7)XI10a	12.2(33)SB2（2008年9月26日に入手可能）
12.3XJ	脆弱性なし	
12.3XK	脆弱性なし	
12.3XL	脆弱性なし	
12.3XQ	脆弱性なし	
12.3XR	脆弱性なし	
12.3XS	脆弱性なし	
12.3XU	脆弱性なし	
12.3XW	脆弱性なし	
12.3XX	脆弱性なし	
12.3XY	脆弱性なし	
12.3XZ	脆弱性なし	
12.3YA	脆弱性なし	
12.3YD	脆弱性なし	

12.3YF	脆弱性なし	
12.3YG	脆弱性なし	
12.3YH	脆弱性なし	
12.3YI	脆弱性なし	
12.3YJ	脆弱性なし	
12.3YK	脆弱性なし	
12.3YM	脆弱性なし	
12.3YQ	脆弱性なし	
12.3YS	脆弱性なし	
12.3YT	脆弱性なし	
12.3YU	脆弱性なし	
12.3YX	脆弱性なし	
12.3YZ	脆弱性なし	
12.3ZA	脆弱性なし	
Affected 12.4-Based	First Fixed Release（修正された最初のリリース）	推奨リリース

Releases		
12.4	注：12.4(3)より前のリリースには脆弱性があり、12.4(3)以降のリリースには脆弱性はありません。	12.4(18c)
12.4JA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JMC	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	脆弱性なし	
12.4SW	脆弱性なし	
12.4T	脆弱性なし	

12.4XA	脆弱性なし	
12.4XB	脆弱性なし	
12.4XC	脆弱性なし	
12.4XD	脆弱性なし	
12.4XE	脆弱性なし	
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性なし	
12.4XK	脆弱性なし	
12.4XL	脆弱性なし	
12.4XM	脆弱性なし	
12.4XN	脆弱性なし	
12.4XP	脆弱性なし	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	

12.4XT	脆弱性なし	
12.4XV	脆弱性なし	
12.4XW	脆弱性なし	
12.4XY	脆弱性なし	
12.4XZ	脆弱性なし	
12.4YA	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発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc

改訂履歴

リビジョン 1.1	2009年4月16日	現在は古くなっているため、結合されたソフトウェアテーブルへの参照を削除
リビジョン 1.0	2008年9月24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。