Cisco IOS NAT Skinny Call Control Protocolの脆弱性

High

アドバイザリーID : cisco-sa-20080924-sccp
初公開日 : 2008-09-24 16:00
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCsi17020 CSCse81684 CSCsg22426

CVE-2008-3810
CVE-2008-3811

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

一連のセグメント化されたSkinny Call Control Protocol(SCCP)メッセージにより、ネットワークアドレス変換(NAT)SCCPフラグメンテーションサポート機能が設定されたCisco IOSデバイスがリロードする場合があります。

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-sccp 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-cucm
- 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-iosips

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-l2tp
- 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-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-sip
- 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-ubr
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn

該当製品

脆弱性のある製品

このセキュリティアドバイザリは、NAT用に設定され、NAT SCCPフラグメンテーションサポート機能をサポートするCisco IOSソフトウェアを実行するすべてのシスコ製品に適用されます。この機能は、Cisco IOSバージョン12.4(6)Tで初めて導入されました。

Cisco IOSデバイスにログインしてNATが有効になっているかどうかを確認し、show ip nat statisticsコマンドを発行します。次の例は、NATが設定されたデバイスを示しています。

<#root>

```
Router#
show ip nat statistics


Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool mypool refcount 2
 pool mypool: netmask 255.255.255.0
        start 192.168.10.1 end 192.168.10.254
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

または、show running-config | include ip natコマンドを使用して、ルータインターフェイスでNATが有効になっているかどうかを確認します。

注：NATに関して、「内部」という用語は変換されるネットワークを指します。このドメインの内部では、ホストは1つのアドレス空間にアドレスを持ち、「外部」では、NATが設定されると、ホストは別のアドレス空間にアドレスを持つように見えます。最初のアドレス空間はローカルアドレス空間と呼ばれ、2番目のアドレス空間はグローバルアドレス空間と呼ばれます。NATをイネーブルにするには、ip nat insideおよびip nat outsideインターフェイスコマンドが、対応するルータインターフェイス上に存在している必要があります。

Cisco IOS製品で稼働しているソフトウェアを判別するには、デバイスにログインし、show versionコマンドを発行してシステムバナーを表示します。Cisco IOSソフトウェアは、「Internetwork Operating System Software」または単に「IOS」と表示されます。 出力の次の行では、カッコ内にイメージ名が表示され、その後に「Version」とCisco IOSリリース名が続きます。他のシスコデバイスにはshow versionコマンドがないか、異なる出力が返されます。

次の例は、IOSイメージが稼働しているデバイスからの出力結果を示しています。

```
<#root>

router>

show version

Cisco IOS Software, 7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(6)T2, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 16-May-06 16:09 by kellythw
<more output removed for brevity>
```

脆弱性を含んでいないことが確認された製品

Cisco IOS XRおよびIOS XEはこの脆弱性の影響を受けません。

NATが明示的に設定されていないCisco IOSデバイスには脆弱性は存在しません。

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

Skinny Call Control Protocol(SCCP)は、SCCPクライアントとCall Manager(CM)間の音声通信を可能にします。通常、CMはデフォルトでTCPポート2000のSCCPクライアントにサービスを提供します。最初に、SCCPクライアントはTCP接続を確立することによってCMに接続します。また、可能であれば、クライアントはセカンダリCMとのTCP接続も確立します。

NAT SCCPフラグメンテーションサポート機能は、NAT Skinny Application Layer Gateway(ALG)がSkinny制御メッセージを再構成できるため、TCPセグメンテーションシナリオでSkinny制御メッセージの交換が失敗することを防ぎます。IPまたはポート変換を必要とするセグメント化されたペイロードはドロップされなくなります。NAT SCCPフラグメンテーションサポート機能は、Cisco IOSバージョン12.4(6)Tで導入されました。

フラグメント化された一連のSCCPメッセージにより、NAT SCCP Fragmentation Support機能を実行しているCisco IOSルータがリロードする場合があります。

この脆弱性は、Cisco Bug ID CSCsg22426（登録ユーザ専用）およびCSCsi17020(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2008-3810およびCVE-2008-3811が割り当てられています。

回避策

回避策として、管理者は次の例に示すように、no ip nat service skinny tcp port 2000コマンドを使用してSCCP NATサポートを無効にすることができます。

<#root>

```
Router(config)#
no ip nat service skinny tcp port 2000
```

注：Cisco CallManagerでSkinnyシグナリング用にデフォルトポート(2000)と異なるTCPポートを使用している場合、このコマンドを適宜調整する必要があります。

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
該当する 12.0 ベースのリリースはありません。		
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	脆弱性なし	
12.2SBC	脆弱性なし	
12.2SCA	脆弱性なし	
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	脆弱性なし	
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	脆弱性なし	
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
該当する 12.3 ベースのリリースはありません。		
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	脆弱性なし	
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	12.4(11)MD4	12.4(15)MD1
12.4MR	12.4(16)MR	12.4(19)MR
12.4SW	12.4(15)SW2（2008年9月28日に入手可能）	12.4(15)SW2（2008年9月28日に入手可能）
12.4T	12.4(11)T4 12.4(15)T2 12.4(20)T 12.4(6)T11 12.4(9)T5	12.4(15)T7

12.4XA	脆弱性なし	
12.4XB	脆弱性なし	
12.4XC	脆弱性あり(最初の修正は12.4T)	12.4(15)T7
12.4XD	脆弱性なし	
12.4XE	脆弱性あり(最初の修正は12.4T)	12.4(15)T7
12.4XF	脆弱性あり(最初の修正は12.4T)	12.4(15)T7
12.4XG	12.4(9)XG3	12.4(9)XG3
12.4XJ	脆弱性あり(最初の修正は12.4T)	12.4(15)T7
12.4XK	脆弱性あり(最初の修正は12.4T)	12.4(15)T7
12.4XL	12.4(15)XL2	12.4(15)XL2
12.4XM	12.4(15)XM1	12.4(15)XM1
12.4XN	脆弱性あり。TACに連絡	
12.4XP	脆弱性あり。TACに連絡	

12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性あり(最初の修正は12.4T)	12.4(15)T7
12.4XV	脆弱性あり。TACに連絡	
12.4XW	12.4(11)XW7	12.4(11)XW9
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。

URL

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

改訂履歴

リビジ	2009年4月	現在は古くなっているため、結合

ョン 1.1	16日	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	初版リリース

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。