Cisco IOSソフトウェアのNAT Skinny Call Control Protocolの脆弱性

アドバイザリーID : cisco-sa-20100324-sccp
初公開日 : 2010-03-24 16:00
最終更新日 : 2012-09-21 19:10
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCsy09250

CVE-2010-0584

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

巧妙に細工されたSkinny Client Control Protocol(SCCP)メッセージにより、ネットワークアドレス変換(NAT)の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される場合があります。

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-20100324-sccp で公開されています。

注：2010年3月24日のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開には7件のSecurity Advisoryが含まれています。すべてのアドバイザリで Cisco IOS ソフトウェアの脆弱性が取り上げられています。各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。2010 年 3 月 24 日またはそれ以前に公開されたすべての Cisco IOS ソフトウェアの脆弱性に対応したリリースについては、次の URL にある表を参照してください。

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-bundle

個々の公開リンクは、次のリンクの「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar10.html

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、ネットワークアドレス変換(NAT)が設定され、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ソフトウェアが稼働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ソフトウェアリリース12.4(6)Tで初めて導入されました。

Cisco IOSデバイスでNATが有効になっているかどうかを確認するには、デバイスにログインしてコマンドshow ip nat statistics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、show running-config | include ip natコマンドを使用して、デバイスでNATが有効になっているかどうかを確認します。

NATの従来の設定では、「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。

NAT 仮想インターフェイス (NVI) 機能により、NAT 内部または NAT 外部としてインターフェイスを設定する必要性がなくなります。デバイスがNVI用に設定されている場合は、次の例に示すように、ユーザEXECモードまたは特権EXECモードでshow ip nat nvi statisticsコマンドを使用できます。

<#root>

```
Router#
show ip nat nvi statistics


Total active translations: 0 (0 static, 0 dynamic; 0 extended) NAT Enabled interfaces:
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0 Expired translations: 0 Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pool1 refcount 1213 pool pool1: netmask 255.255.255.0
         start 192.168.1.10 end 192.168.1.253
         start 192.168.2.10 end 192.168.2.253
         start 192.168.3.10 end 192.168.3.253
         start 192.168.4.10 end 192.168.4.253
         type generic, total addresses 976, allocated 222 (22%), misses 0


!---output truncated
```

Cisco IOS製品で実行されているソフトウェアを確認するには、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。

<#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

!---output truncated
```

脆弱性を含んでいないことが確認された製品

Cisco IOS XRソフトウェアおよびIOS XEソフトウェアは、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 Client 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を使用すると、Skinny Application Layer Gateway(ALG)でSkinny制御メッセージを再構成できます。この機能はCisco IOSバージョン12.4(6)Tで導入されたため、リアセンブルとNATを必要とするSCCPペイロードは廃棄されなくなりました。

一連の巧妙に細工されたSCCPパケットにより、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 CSCsy09250 (登録ユーザ専用)として文書化され、CVE IDとしてCVE-2010-0584が割り当てられています。

回避策

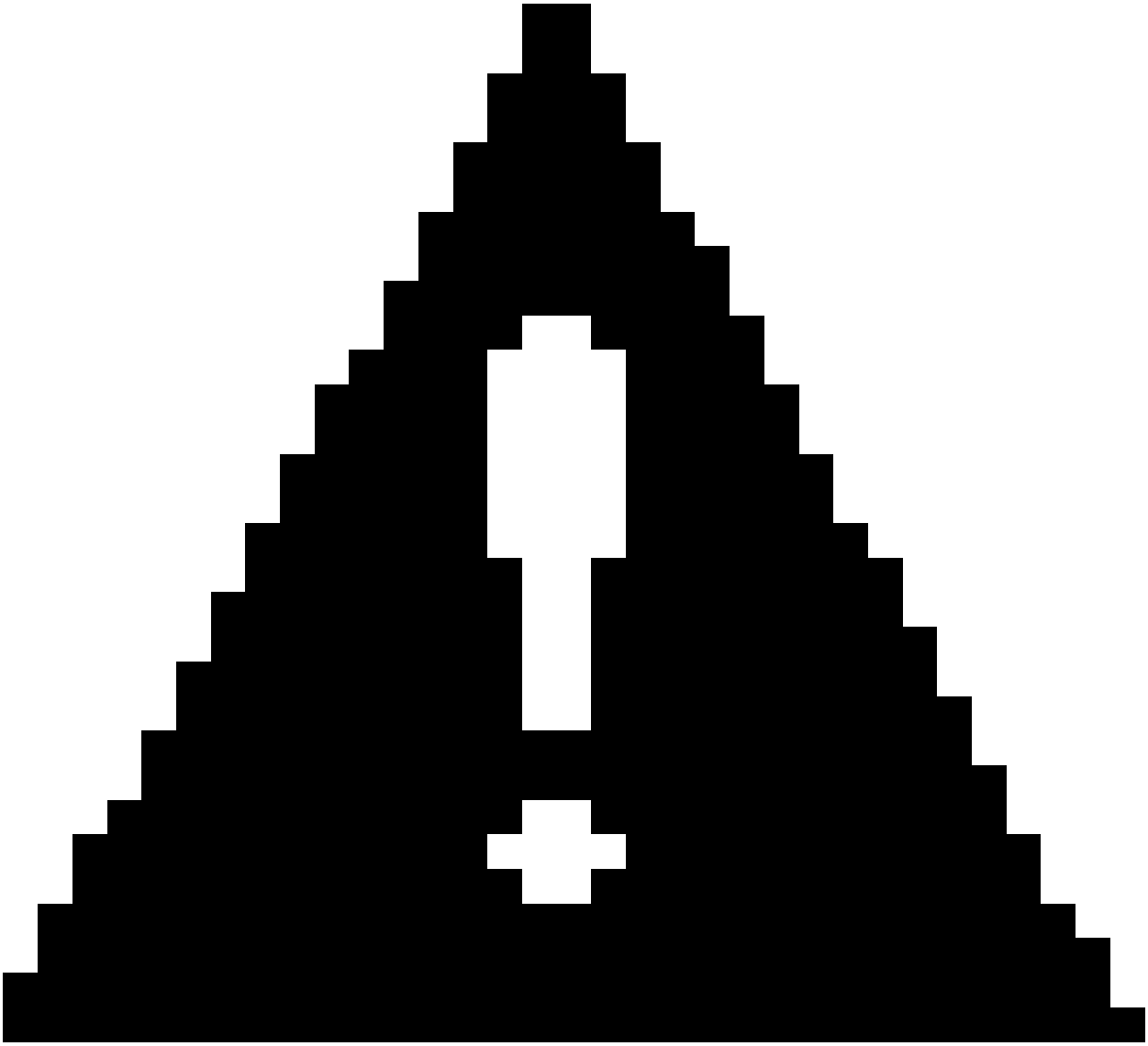
回避策として、管理者は次の例に示すように、no ip nat service skinny tcp port 2000コマンドを使用してSCCP NATサポートを無効にすることができます。

```
<#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。



注意：この回避策を適用できるのは、SCCPトラフィックをNATで処理する必要がないネットワークだけです。この回避策を実施する前に確認してください。

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。[バンドルの最初の修正リリース（Bundle First Fixed Release）] 列は、この Cisco IOS セキュリティ アドバイザリ バンドル資料に記載されているすべての公開された脆弱性に対する修正がある最も古い利用可能なリリースを示しています。可能な場合は、利用可能な最新のリリースにアップグレードすることをお勧めします。

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	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
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	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
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	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
影響を受ける 12.2 ベースのリリースはありません。		
Affected 12.3-Based Releases	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース

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	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
12.4	脆弱性なし	12.4(25c) 15.0(1)M1
12.4GC	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JA	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JDA	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JDC	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクシ

		ョンの手順に従って、サポート組織にお問い合わせください
12.4JDD	脆弱性なし	12.4(10b)JDD1
12.4JHA	脆弱性なし	脆弱性なし
12.4JK	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JL	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JMA	脆弱性なし	12.4(3g)JMA2 より前のリリースには脆弱性があり、12.4(3g)JMA2 以降のリリースには脆弱性はありません。
12.4JMB	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4JX	脆弱性なし	脆弱性あり(最初の修正

		は12.4JA)
12.4MD	12.4(11)MD10	12.4(24)MD
12.4MDA	12.4(22)MDA2	12.4(22)MDA2
12.4MR	12.4(4)MR1までのリリースには脆弱性はありません。	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4SW	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4T	12.4(20)T4 12.4(22)T3 12.4(15)T10 12.4(24)T2	12.4(15)T12 12.4(20)T5 12.4(24)T3（2010年3月26日に入手可能） 12.4(22)T4
12.4XA	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XB	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行

		してください。
12.4XC	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XD	脆弱性なし	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XE	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XF	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XG	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XJ	脆弱性あり。	脆弱性あり。15.0Mの任

	15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	意のリリースまたは修正済み12.4リリースに移行してください。
12.4XK	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XL	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XM	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XN	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください

12.4XP	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XQ	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XR	12.4(22)XR3	12.4(22)XR3
12.4XT	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XV	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XW	脆弱性あり。15.0Mの任意のリリースまたは修正	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行

	済み12.4Tリリースに移行してください。	してください。
12.4XY	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4XZ	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4YA	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4Tリリースに移行してください。	脆弱性あり。15.0Mの任意のリリースまたは修正済み12.4リリースに移行してください。
12.4YB	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4YD	脆弱性あり。このアドバイザリの「修正済みソフトウ	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクシ

	エアの取得」セクションの手順に従って、サポート組織にお問い合わせください	ョンの手順に従って、サポート組織にお問い合わせください
12.4YE	12.4(22)YE2	12.4(22)YE2 12.4(24)YE
12.4YG	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
影響を受ける 15.0 ベースのリリース	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
影響を受ける 15.0 ベースのリリースはありません。		
影響を受ける 15.1 ベースのリリース	このアドバイザリの最初の修正リリース	2010 年 3 月 24 日のバンドル資料に記載されているすべてのアドバイザリの最初の修正リリース
影響を受ける 15.1 ベースのリリースはありません。		

Cisco IOS XE ソフトウェア

IOS XE リリース	First Fixed Release（修正された最初のリリース）
2.1.x	脆弱性なし
2.2.x	脆弱性なし
2.3.x	脆弱性なし
2.4.x	脆弱性なし
2.5.x	脆弱性なし
2.6.x	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。この脆弱性はカスタマー サービス リクエストの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-sccp

改訂履歴

リビジョン 1.0	2010 年 3 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。