Cisco IOS NAT Skinny Call Control Protocol（SCCP）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 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）SCCP フラグメンテーション サポート 機能でリロードするために設定される Cisco IOSデバイスを引き起こすかもしれません。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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 924-sccp で掲示されます。

注: 2008 年 9月 24 日 IOS アドバイザリによって組み込まれる書は 12 のセキュリティ アドバイザリが含まれています。 アドバイザリの 11 は Cisco の IOS software の脆弱性に対処し、1 つのアドバイザリは Cisco Unified Communications Manager の脆弱性に対処します。 各アドバイザリはリリースをリストしますアドバイザリに説明がある脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- 924-cucm
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosfw
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosips
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc
- 924-l2tp
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-

multicast
- 924-sccp
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn

該当製品

脆弱性のある製品

この Security Advisory は NAT のために設定される Cisco IOSソフトウェアを実行する NAT SCCP フラグメンテーション サポート 機能をサポートし、すべてのシスコ製品に適用します。 この機能は Cisco IOSバージョン 12.4(6)T で最初に導入されました。

NAT が Cisco IOSデバイスでログイン する デバイスに有効に なる コマンド **show ip nat statistics** を発行すればかどうか確認するために。 次の例は NAT で設定されるデバイスを示したものです:

```
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** を使用できます | NAT がルータ インターフェイスで有効に なったかどうか確認する **ip nat コマンドを含んで下さい**。

注: NAT について、条件「内部」は変換されるそれらのネットワークを示します。 このドメインの中で、NAT が設定される場合「外部で」、別のアドレス スペースのアドレスがあるようであるが、ホストに 1 つのアドレス スペースのアドレスがあります。 最初のアドレス スペースはローカルアドレス空間と言われ、第 2 はグローバルアドレス空間と言われます。 **ip nat inside** および **ip nat outside interface コマンドは**有効に なるべき NAT のために対応した ルータ インターフェイスにある必要があります。

ソフトウェアを判別するためにデバイスに Cisco IOS 製品で、ログイン動作するシステムバナーを表示する show version コマンドを発行すれば。 Cisco IOSソフトウェアは「インターネットワーク オペレーティング システム ソフトウェア」として識別しますそれ自身をまたは単に「IOS」。 出力次の行、「バージョンに」先行しているかっこと Cisco IOS リリース名前間のイメージ名 ディスプレイ。 他の Ciscoデバイスに show version コマンドがありませんし、別

の出力を与えないために。

次の例は IOSイメージを実行するデバイスからの出力を示したものです:

```
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 はこの脆弱性から影響を受けません。

明示的に NAT のために設定されない Cisco IOSデバイスは脆弱ではないです。

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）間の音声通信を有効に します。 通常、CM は TCPポート 2000 年で SCCP クライアントにサービスをデフォルトで提供します。 最初に、SCCP クライアントは CM に TCP 接続の確立によって接続します; クライアントはまたセカンダリ CM の TCP 接続を、もし可能であれば確立します。

NAT SCCP フラグメンテーション サポート 機能は TCP セグメンテーション シナリオに失敗から NAT スキニー アプリケーション層ゲートウェイ（ALG）がスキニー コントロールメッセージを再構成できるのでスキニー制御メッセージ交換を防ぎます。 IP か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もはや廃棄されません。 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。

一連のフラグメント化された SCCP メッセージにより Cisco IOS ルータを引き起こすかもしれませんリロードするために NAT SCCP フラグメンテーション サポート 機能を実行している。

この脆弱性は Cisco バグ ID CSCsg22426（登録ユーザのみ）および CSCsi17020（登録ユーザのみ）で文書化されています、CVE 識別 CVE-2008-3810 および CVE-2008-3811 を割り当てられました。

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 サービス スキニー TCPポート 2000** コマンドを使用して SCCP NAT サポートを、ディセーブルにすることができます:

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

注: Cisco Unified CallManager がデフォルトポートと別のスキニー シグナリングのために TCPポートを使用すれば（2000）、このコマンドをそれに応じて調節する必要があります。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

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	**修理されたリリースの Â Â Â Â Â 可用性**	
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; 28-SEP-08 で利用可能	12.4(15)SW2; 28-SEP-08 で利用可能
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; first fixed in 12.4T	12.4(15)T7
12.4XD	脆弱性なし	
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XF	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XG	12.4(9)XG3	12.4(9)XG3
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XK	脆弱性あり; first fixed in 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; contact TAC	
12.4XP	脆弱性あり; contact TAC	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XV	脆弱性あり; contact TAC	
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	

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sccp

改訂履歴

リビジョン 1.1	2009-April-16	現在旧式であるように、結合されたソフトウェア テーブルへの取除かれた参照
リビジョン 1.0	2008-September-24	初版リリース

利用規約