Cisco IOSソフトウェア モバイル IP およびモービル IPv6 脆弱性

High	**アドバイザリーID :** cisco-sa-20090325-mobileip **初公開日 :** 2009-03-25 16:00 **バージョン 1.3 :** Final **CVSSスコア :** 7.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCsm97220 CSCso05337	CVE-2009-0634 CVE-2009-0633

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 IOSソフトウェアを実行しているおよびモバイル IP ネットワーク アドレス変換（NAT）走査機能のために設定されてまたはモービル IPv6 はブロックされたインターフェイスという結果に終るかもしれないサービス拒絶（DoS）攻撃に脆弱ですデバイス。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。

このアドバイザリは次のリンク
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip
で掲示されます。

注: 2009 年 3月 25 日、Cisco IOS セキュリティ アドバイザリによって組み込まれる書は 8 つのセキュリティ アドバイザリが含まれています。 アドバイザリすべては Cisco IOSソフトウェア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の脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCP サービス拒否の脆弱性
  325-ctcp

- Cisco IOSソフトウェア倍数は IP ソケット脆弱性を特色にします
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- Cisco IOSソフトウェア モバイル IP およびモービル IPv6 脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip

- Cisco IOSソフトウェア Secure Copy（SCP） 特権 拡大脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp

- Cisco IOSソフトウェア Session Initiation Protocol（SIP） サービス拒否の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

- Cisco IOSソフトウェア複数の機能によって細工 される TCP シーケンス脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- Cisco IOSソフトウェア複数の機能 巧妙に細工された UDP パケットの脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

- Cisco IOSソフトウェア WebVPN および SSLVPN 脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

影響を受けたバージョンを Cisco IOSソフトウェアのおよび設定されるモバイル IP NAT 走査機能かモービル IPv6 のために実行しているデバイスは脆弱です。

脆弱性のある製品

Cisco IOSソフトウェアを実行し、モバイル IP NAT 横断機能のために設定されたデバイスは **show running-config コマンド**の出力の次と同じようなラインを備えています:

```
ip mobile home-agent nat traversal [...]
```

または

```
ip mobile foreign-agent nat traversal [...]
```

または

```
ip mobile router-service collocated registration nat traversal [...]
```

Cisco IOSソフトウェアを実行し、モービル IPv6 のために設定されたデバイスは **show running-config コマンド**の出力の次と同じようなラインを備えています:

```
ipv6 mobile home-agent
```

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "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 デバイスでは、**show version** コマンドが存在しなかったり、別の出力が表示されたりします。

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:

```
    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 C1841-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T を実行している Cisco製品を指定したものです:

```
    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 ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/warp/public/620/1.html。

脆弱性を含んでいないことが確認された製品

Cisco IOS XR はこれらの脆弱性から影響を受けません。

Cisco IOS XE はこれらの脆弱性から影響を受けません。

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

モバイル IP は IPv4 および IPv6 両方規格の一部です。 モバイル IP はデバイスがからへの別のもの物理的 な 接続点を 1 つのネットワーク移動するかもしれないのにホストデバイスが単一 IP アドレスによって識別されるようにします。 異なるネットワークの間の移動に関係なく、異なるポイントの接続はユーザ 介入なしでシームレスに実現します。 有線ネットワークからのワイヤレスまたはワイドエリア ネットワークへのローミングはまた可能性のあるです。

モービル IPv6 に関する詳細は次のリンクで見つけることができます:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mobile.html

モバイル IP サポート NAT 横断機能は RFC 3519 で文書化されています。 それはモバイル IP データトラフィックをトンネル伝送する代替方式をもたらします。 モバイル IP 登録要求および応答メッセージの新しい拡張機能はユーザ データグラム プロトコル（UDP）トンネリングを確立するために追加されました。 この機能は気付アドレス（CoA）のためにプライベート IP アドレス（RFC 1918）または外国代理人を（FAS）その使用 プライベート IP アドレス トンネルを確立し、Home Agent （HA）からのモバイルノード（MN）データトラフィックを持つネットワークアドレス変換可能なルータを横断するのに使用する配列されたモードのモバイルデバイスを可能にします。

モバイル IP NAT 走査機能に関する詳細は次のリンクで見つけることができます:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtnatmip.html

影響を受けたバージョンを Cisco IOSソフトウェアのおよび設定されるモービル IPv6 かモバイル IP NAT 走査機能のために実行しているデバイスは DoS 脆弱性から影響を受けます。 システムが再始動されるまでこの脆弱性の不正利用の成功によりインターフェイスはトラフィックを処理することを停止します可能性があります。 おこるパケットは正常なエクスプロイトのためのルータに向かう必要があります。

これらの脆弱性 Cisco バグ ID **CSCsm97220**（登録ユーザのみ）および **CSCso05337**（登録ユーザのみ）で文書化されています、よくある脆弱性および公開（CVE） ID CVE-2009-0633 および CVE-2009-0634 は割り当てられました。

回避策

次の軽減および識別 メソッドはこれらの脆弱性のために識別されました:

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:

IPv4 例:

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to
RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any access-
list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110
deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-
list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny your space as source from entering your
AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit
BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp
host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses.
access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic.
access-list 110 permit ip any any
```

IPv6 例:

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from
entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !---
Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host
bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses.
deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6
any any
```

ホワイトペーパー 『Protecting Your Core: Infrastructure Protection Access Control Lists (ACL) には、インフラストラクチャ保護アクセス リストに関するガイドラインと推奨配備方法が記載されています。 この白書は次のリンク
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml
で得ることができます

Cisco IOS Embedded Event Manager

インターフェース キューがブロックされたことを Cisco IOS Embedded Event Manager (EEM) ポリシーにより検知することができます。 EEM は Cisco IOS デバイスにおけるイベント検知と対応アクション機能を提供します。 EEM は 管理者に対してインターフェースがブロックされたことを email, syslog メッセージ または Simple Network Management Protocol (SNMP) trap により警告することができます。

インターフェースがブロックされたことを管理者に syslog で警告することができるサンプル EEM ポリシーを EEM 専門のオンラインコミュニティ Cisco Beyond で入手することが出来ます。 サンプル スクリプトは次のリンクで入手可能です:

http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=981

EEM についての追加情報は、次の Cisco.com へのリンクより入手可能です:
http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

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**
該当する 12.2 基づいたリリースがありません		

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	脆弱性なし	
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	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
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	脆弱性なし	
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	Release prior to 12.3(11)YK3 are vulnerable， releases 12.3(11)YK3 and later are not vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YM	12.3(14)YM13	12.3(14)YM13
12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YS	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YU	脆弱性あり; 12.4T への移行する	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YX	Release prior to 12.3(14)YX10 are vulnerable， releases 12.3(14)YX10 and later are not vulnerable;	12.3(14)YX14
12.3YZ	脆弱性なし	
12.3ZA	脆弱性なし	
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(18e) 12.4(23a); 05-JUN-2009 で利用可能	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能

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	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	12.4(19)MR	12.4(19)MR2
12.4SW	脆弱性なし	
12.4T	12.4(20)T 12.4(15)T8 12.4(15)T9; 29-APR-2009 で利用可能	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XB	12.4(15)T8 12.4(20)T 12.4(15)T9; 29-APR-2009 で利用可能	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XC	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XD	12.4(4)XD12; 27-MAR-2009 で利用可能	12.4(4)XD12; 27-MAR-2009 で利用可能
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XF	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XG	脆弱性なし	
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9

		; 29-APR-2009 で利用可能
12.4XK	脆弱性なし	
12.4XL	12.4(15)XL4	12.4(15)XL4
12.4XM	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XN	脆弱性あり; contact TAC	
12.4XP	脆弱性あり; contact TAC	
12.4XQ	12.4(15)XQ2	12.4(15)XQ2
12.4XR	12.4(15)XR4	12.4(22)T1
12.4XT	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XV	脆弱性あり; contact TAC	
12.4XW	12.4(11)XW10	12.4(11)XW10
12.4XY	12.4(15)XY4	12.4(22)T1 12.4(15)T9 ; 29-APR-2009 で利用可能
12.4XZ	12.4(15)XZ1	12.4(15)XZ2
12.4YA	脆弱性なし	
12.4YB	脆弱性なし	
12.4YD	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。

この脆弱性は、お客様 によって Cisco に報告されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip

改訂履歴

リビジ	2009-	March/09 によって結合される修正

ョン 1.3	June-25	済みソフトウェア 表への取除かれた参照。
リビジョン 1.2	2009-June-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。
リビジョン 1.1	2009-May-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。
リビジョン 1.0	2009-Mar-25	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。