Cisco Security Advisory: IPv6 Routing Header Vulnerability

Advisory ID: cisco-sa-20070124-IOS-IPv6

http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

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。

Revision 1.2

Last Updated 2007 May 04 1600 UTC (GMT)

For Public Release 2007 January 24 1600 UTC (GMT)

目次

要約

特定の不正な IPv6 Type 0 Routing ヘッダを処理することにより、Cisco IOS が稼動する機器がクラッシュすることがあります。この脆弱性は Mobile IPv6 の環境で使用される IPv6 Type 2 Routing ヘッダでは影響を受けません。IPv6 は Cisco IOS においてはデフォルトでは有効になっていません。

シスコは本脆弱性の影響を受けるお客様のために、本脆弱性対処用のソフトウェアを無償で提供しています。

この脆弱性に対しては、影響を緩和するための回避策があります。回避策は Mobile IPv6 の使用状況と現在どの Cisco IOS バージョンをご利用になっているかに依存します。

本脆弱性は当初顧客使用環境で報告され、その発生トリガについては脆弱性の修正過程で発見されています。

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

該当製品

Cisco IOS を稼動させている機器で、少なくとも 1 つのインターフェイスにて IPv6 を有効にしている場合にこの脆弱性による影響がある可能性があります。

脆弱性が存在する製品

シスコ製品で稼働中のソフトウェアを確認するには、機器にログインして **show version** コマンドを実行し、システムバナーを画面に表示します。Cisco IOS ソフトウェアは「Internetwork Operating System Software」もしくは単に「IOS」と表示します。そのすぐ後ろにイメージ名が括弧の間に 表示され (場合により改行されています) 、続いて「Version」と IOS リリース名が表示されます。 (IOS 以外の) 他のシスコ製品は **show version** コマンドがない場合や、異なる表示をする場合があります。

次の例は、シスコ製品で IOS リリース 12.4(9.10) が稼動していることを示しています。

```
Cisco IOS Software, 7200 Software (C7200-JK9O3S-M), Version 12.4(9.10), INTERIM
SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 29-May-06 04:42 by prod_rel_team
```

Cisco IOS の命名に関する更なる情報は以下の URL を参照してください。
http://www.cisco.com/warp/public/620/1.html

脆弱性が存在しない製品

上記以外のシスコ製品において本アドバイサリの影響を受けるものは確認されていません。特に、Cisco IOS XR、Cisco PIX アプライアンス製品、Cisco MDS 9000 シリーズはいずれも本アドバイサリによる影響を受けません。

Top of the section Close Section

詳細

本脆弱性は Cisco IOS が不正な IPv6 Type 0 Routing ヘッダを処理するときのみ発生します。これらは Source Routing 使用時に使われます。Source Routing は、パケットが宛先に至るための経路を送信元が明示的に指定する方法です。Source Routing は、Cisco IOS 上に IPv6 が設定されている場合はデフォルトで有効になります。この脆弱性を発生させるためには、パケットはその機器上に定義されたいずれかの IPv6 アドレスに対して送信される必要があります。脆弱性は IP レイヤ上に存在するため、TCP、ICMP、UDP 等のパケットタイプには依存しません。このため本脆弱性に対する対処を適用する際には、偽装されたパケットによって影響を受ける点に注意をはらう必要があります。

IPv6 Multicast パケットは本脆弱性による影響を受けません。

Type 0 Routing ヘッダに加え、IPv6 は Mobile IPv6 環境にて使用される Type 2 Routing もサポートされていますが、 Type 2 Routing ヘッダは本脆弱性の影響を受けません。

脆弱性を有する Cisco IOS ソフトウェアを稼動しているルータは、IPv6 パケット内の宛先アドレスがいずれかのインターフェイスに定義された IPv6 アドレスである場合のみ、Type 0 Routing ヘッダを持つパケットの処理が発生します。このアドレスはグローバル、ループバック、または

リンク ローカルのいずれでも構いません。リンク ローカル アドレスは外部にルーティングされないアドレスであるため、直接接続された機器間のみに有効です。

IPv6 パケットが IPv4 ネットワークをトンネリングされるような構成においても、脱カプセル化（Decapsulation）後の IPv6 宛先アドレスがその機器上の IPv6 アドレスのいずれかであるような場合は影響をうける可能性があります。これはカプセル化（Encapsulation）の方法自体（MPLS、GRE、IPv6 in IPv4）とは無関係に起こりえます。

この脆弱性は Cisco Bug ID CSCsd40334（ 登録ユーザのみ ）および CSCsd58381（ 登録ユーザのみ ）として文書化されています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供いたします。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

Cisco PSIRT は重み付けパラメータ（Impact Bias）を全て Normal に設定しています。お客様はこれらの重み付けパラメータを利用し、特定の脆弱性の影響を確認することを推奨いたします。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する手助けとなる標準ベースの評価法です。

シスコは次の URL にて CVSS に関する FAQ を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。 http://intellishield.cisco.com/security/alertmanager/cvss

(customers only)						
CVSS Base Score - **10**						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - **8.3**						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

(customers only)						
CVSS Base Score - **10**						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Rem	Low	Not	Complet	Comp	Compl	Nor

ote		Required	e	lete	ete	mal
CVSS Temporal Score - **8.3**						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

Top of the section Close Section

影響

脆弱性の利用に成功した場合、一部のメモリ構造を破壊する恐れがあります。多くの場合、これは機器のクラッシュを誘発し、継続的な攻撃により結果的にサービス妨害攻撃（DoS）に発展する可能性がありますが、 メモリ構造破壊によって不正コードが実行される可能性があります。リモート コードの実行が成功した場合、機器の完全性は完全に失われます。

Top of the section Close Section

ソフトウェア バージョンおよび修正

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/ および本アドバイザリ以降に公開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デバイス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。情報が不明確な場合は、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

以下の Cisco IOS ソフトウェアの表の各行は、対象となるリリース トレイン、プラットフォームおよび製品群を示します。あるリリーストレインが脆弱である場合、修正が組み込まれている最も早いリリース（最初に修正されたリリース）とそれが利用可能となる予定日が「Rebuild」および「Maintenance」の列に示されます。実行しているリリースが、そのトレインで「First Fixed Release」よりも前のものである機器は脆弱であることが知られています。使用するリリースは少なくとも示されたリリース以降へアップグレードすることが推奨されます。

「Rebuild」および「Maintenance」の用語に関する情報は以下をご参照ください。
http://www.cisco.com/warp/public/620/1.html

注意：2007 年 1 月 24 日に 3 つの IOS 関連の Security Advisory と 1 つの Field Notice が発行されます。個々のアドバイサリはそのアドバイサリ内の問題を解決するリリースについてのみ記載しています。全ての修正が含まれたソフトウェア一覧は、
http://www.cisco.com/warp/public/707/cisco-sa-20070124-bundle.shtml にて確認できます。 ここでは 3 つ全ての脆弱性に対応するソフトウェアリリースを選択することができます。1 月 24 日に発行されるアドバイサリ及び Field Notice は以下の通りです。

- http://www.cisco.com/warp/public/707/cisco-amb-20070124-IOS-IPv6.shtml
- http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml
- http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml
- http://www.cisco.com/warp/public/770/fn62613.shtml

サマータイム（DST）の変更を含むソフトウェア リビルドは 2007 年 3 月に提供されます。これについてのリクエストは Technical Assistance Center（TAC）まで直接お問い合わせください。その際にこのアドバイサリをリファレンスとしてご利用ください。

Major Release	Availability of Repaired Releases

Affected 12.0-Based Releases	Rebuild	Maintenance
12.0	Not vulnerable	
12.0DA	Not vulnerable	
12.0DB	Not vulnerable	
12.0DC	Not vulnerable	
12.0S	12.0(32)S3	
12.0SC	Not vulnerable	
12.0SL	Not vulnerable	
12.0SP	Not vulnerable	
12.0ST	Vulnerable; migrate to 12.0(32)S3 or later	
12.0SX	Vulnerable for only 12.0(30)SX; contact TAC	
12.0SY		12.0(32)SY
12.0SZ	Vulnerable; migrate to 12.0(32)S3 or later	
12.0T	Not vulnerable	
12.0W	Not vulnerable	
12.0WC	Not vulnerable	
12.0WT	Not vulnerable	
12.0XA	Not vulnerable	
12.0XB	Not vulnerable	
12.0XC	Not vulnerable	
12.0XD	Not vulnerable	
12.0XE	Not vulnerable	
12.0XF	Not vulnerable	
12.0XG	Not vulnerable	
12.0XH	Not vulnerable	
12.0XI	Not vulnerable	
12.0XJ	Not vulnerable	
12.0XK	Not vulnerable	
12.0XL	Not vulnerable	
12.0XM	Not vulnerable	
12.0XN	Not vulnerable	
12.0XQ	Not vulnerable	
12.0XR	Not vulnerable	
12.0XS	Not vulnerable	
12.0XV	Not vulnerable	
12.0XW	Not vulnerable	
Affected 12.1-Based Releases	Rebuild	Maintenance
12.1	Not vulnerable	

12.1AA	Not vulnerable
12.1AX	Not vulnerable
12.1AY	Not vulnerable
12.1AZ	Not vulnerable
12.1CX	Not vulnerable
12.1DA	Not vulnerable
12.1DB	Not vulnerable
12.1DC	Not vulnerable
12.1E	Not vulnerable
12.1EA	Not vulnerable
12.1EB	Not vulnerable
12.1EC	Not vulnerable
12.1EO	Not vulnerable
12.1EU	Not vulnerable
12.1EV	Not vulnerable
12.1EW	Not vulnerable
12.1EX	Not vulnerable
12.1EY	Not vulnerable
12.1EZ	Not vulnerable
12.1T	Not vulnerable
12.1XA	Not vulnerable
12.1XB	Not vulnerable
12.1XC	Not vulnerable
12.1XD	Not vulnerable
12.1XE	Not vulnerable
12.1XF	Not vulnerable
12.1XG	Not vulnerable
12.1XH	Not vulnerable
12.1XI	Not vulnerable
12.1XJ	Not vulnerable
12.1XL	Not vulnerable
12.1XM	Not vulnerable
12.1XP	Not vulnerable
12.1XQ	Not vulnerable
12.1XR	Not vulnerable
12.1XS	Not vulnerable
12.1XT	Not vulnerable
12.1XU	Vulnerable; migrate to 12.3(18) or later
12.1XV	Vulnerable; migrate to 12.3(18) or later
12.1XW	Not vulnerable
12.1XX	Not vulnerable

12.1XY	Not vulnerable	
12.1XZ	Not vulnerable	
12.1YA	Not vulnerable	
12.1YB	Vulnerable; migrate to 12.3(18) or later	
12.1YC	Vulnerable; migrate to 12.3(18) or later	
12.1YD	Vulnerable; migrate to 12.3(18) or later	
12.1YE	Not vulnerable	
12.1YF	Not vulnerable	
12.1YH	Not vulnerable	
12.1YI	Not vulnerable	
12.1YJ	Not vulnerable	
Affected 12.2-Based Releases	**Rebuild**	**Maintenance**
12.2	Not vulnerable	
12.2B	Vulnerable; migrate to 12.3(4)T13 or later	
12.2BC	Vulnerable; migrate to 12.3(17b)BC3 or later	
12.2BW	Vulnerable; migrate to 12.3(18) or later	
12.2BY	Vulnerable; migrate to 12.3(4)T13 or later	
12.2BZ	Not vulnerable	
12.2CX	Vulnerable; migrate to 12.3(17b)BC3 or later	
12.2CY	Not vulnerable	
12.2CZ	Not vulnerable	
12.2DA	Not vulnerable	
12.2DD	Vulnerable; migrate to 12.3(4)T13 or later	
12.2DX	Vulnerable; migrate to 12.3(4)T13 or later	
12.2EU	Vulnerable; migrate to 12.2(25)EWA6 or later	
12.2EW	Vulnerable; migrate to 12.2(25)EWA6 or later	
12.2EWA	12.2(25)EWA6	
12.2EX	Not vulnerable	
12.2EY	Not vulnerable	
12.2EZ	Vulnerable; migrate to 12.2(25)SEE1 or later	
12.2FX	Not vulnerable	

12.2FY	Not vulnerable	
12.2FZ	Not vulnerable	
12.2IXA	Vulnerable; migrate to 12.2(18)IXB or later	
12.2IXB	All 12.2IXB releases are fixed	
12.2IXC	All 12.2IXC releases are fixed	
12.2JA	Not vulnerable	
12.2JK	Not vulnerable	
12.2MB	Not vulnerable	
12.2MC	12.2(15)MC2h	
12.2S	12.2(25)S11	12.2(30)S
12.2SB	12.2(28)SB2	12.2(31)SB
12.2SBC	12.2(27)SBC4	
12.2SEA	Vulnerable; migrate to 12.2(25)SEE1 or later	
12.2SEB	Vulnerable; migrate to 12.2(25)SEE1 or later	
12.2SEC	Vulnerable; migrate to 12.2(25)SEE1 or later	
12.2SED	Vulnerable; migrate to 12.2(25)SEE1 or later	
12.2SEE	12.2(25)SEE1	
12.2SEF	12.2(25)SEF1	
12.2SEG	All 12.2SEG releases are fixed	
12.2SG	12.2(25)SG1	12.2(31)SG
12.2SGA	All 12.2SGA releases are fixed	
12.2SO	Not vulnerable	
12.2SRA	All 12.2SRA releases are fixed	
12.2SRB	All 12.2SRB releases are fixed	
12.2SU	Vulnerable; migrate to 12.3(14)T7 or later	
12.2SV	12.2(25)SV3	12.2(26)SV
12.2SW	12.2(25)SW7	
12.2SX	Vulnerable; migrate to 12.2(18)SXD7a or later	
12.2SXA	Vulnerable; migrate to 12.2(18)SXD7a or later	
12.2SXB	Vulnerable; migrate to 12.2(18)SXD7a or later	
12.2SXD	12.2(18)SXD7 a	
12.2SXE	12.2(18)SXE6	
12.2SXF	12.2(18)SXF5	
12.2SY	Vulnerable; migrate to 12.2(18)SXD7a or later	

12.2SZ	Vulnerable; migrate to 12.2(25)S11 or later
12.2T	Vulnerable; migrate to 12.3(18) or later
12.2TPC	Vulnerable; contact TAC
12.2XA	Vulnerable; migrate to 12.3(18) or later
12.2XB	Vulnerable; migrate to 12.3(18) or later
12.2XC	Vulnerable; migrate to 12.3(4)T13 or later
12.2XD	Vulnerable; migrate to 12.3(18) or later
12.2XE	Not vulnerable
12.2XF	Vulnerable; migrate to 12.3(17b)BC3 or later
12.2XG	Vulnerable; migrate to 12.3(18) or later
12.2XH	Vulnerable; migrate to 12.3(18) or later
12.2XI	Vulnerable; migrate to 12.3(18) or later
12.2XJ	Vulnerable; migrate to 12.3(18) or later
12.2XK	Vulnerable; migrate to 12.3(18) or later
12.2XL	Vulnerable; migrate to 12.3(18) or later
12.2XM	Vulnerable; migrate to 12.3(18) or later
12.2XN	12.2(31)XN
12.2XQ	Vulnerable; migrate to 12.3(18) or later
12.2XR	Not vulnerable
12.2XS	Vulnerable; migrate to 12.3(18) or later
12.2XT	Vulnerable; migrate to 12.3(18) or later
12.2XU	Vulnerable; migrate to 12.3(18) or later
12.2XV	Vulnerable; migrate to 12.3(18) or later
12.2XW	Vulnerable; migrate to 12.3(18) or later
12.2YA	Vulnerable; migrate to 12.3(18) or later
12.2YB	Vulnerable; migrate to 12.3(18) or

	later
12.2YC	Not vulnerable
12.2YD	Vulnerable; migrate to 12.3(11)T10 or later
12.2YE	Vulnerable; migrate to 12.2(25)S11 or later
12.2YF	Vulnerable; migrate to 12.3(18) or later
12.2YG	Not vulnerable
12.2YH	Vulnerable; migrate to 12.3(18) or later
12.2YJ	Vulnerable; migrate to 12.3(18) or later
12.2YK	Not vulnerable
12.2YL	Vulnerable; migrate to 12.3(4)T13 or later
12.2YM	Vulnerable; migrate to 12.3(4)T13 or later
12.2YN	Vulnerable; migrate to 12.3(4)T13 or later
12.2YO	Not vulnerable
12.2YP	Not vulnerable
12.2YQ	Vulnerable; migrate to 12.3(4)T13 or later
12.2YR	Vulnerable; migrate to 12.3(4)T13 or later
12.2YS	Vulnerable; migrate to 12.3(4)T13 or later
12.2YT	Vulnerable; migrate to 12.3(18) or later
12.2YU	Vulnerable; migrate to 12.3(4)T13 or later
12.2YV	Vulnerable; migrate to 12.3(4)T13 or later
12.2YW	Vulnerable; migrate to 12.3(4)T13 or later
12.2YX	Vulnerable; migrate to 12.3(14)T7 or later
12.2YY	Vulnerable; migrate to 12.3(4)T13 or later
12.2YZ	Vulnerable; migrate to 12.2(25)S11 or later
12.2ZA	Vulnerable; migrate to 12.2(18)SXD7a or later
12.2ZB	Vulnerable; migrate to 12.3(4)T13 or later

12.2ZC	Not vulnerable	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; migrate to 12.3(18) or later	
12.2ZF	Vulnerable; migrate to 12.3(4)T13 or later	
12.2ZG	Not vulnerable	
12.2ZH	Vulnerable; contact TAC	
12.2ZJ	Vulnerable; migrate to 12.3(4)T13 or later	
12.2ZL	Vulnerable; contact TAC	
12.2ZN	Vulnerable; migrate to 12.3(4)T13 or later	
12.2ZP	Not vulnerable	
Affected 12.3-Based Releases	**Rebuild**	**Maintenance**
12.3	12.3(17b)	12.3(18)
12.3B	Vulnerable; migrate to 12.3(11)T10 or later	
12.3BC	12.3(17b)BC3	
12.3BW	Vulnerable; migrate to 12.3(11)T10 or later	
12.3JA	Not vulnerable	
12.3JEA	All 12.3JEA releases are fixed	
12.3JEB	All 12.3JEA releases are fixed	
12.3JK	Not vulnerable	
12.3JX	Not vulnerable	
12.3T	12.3(4)T13	
	12.3(11)T10	
	12.3(14)T7	
	Limited platform support is available: Contact TAC	
	Please migrate to 12.4(8) or later	
12.3TPC	Not vulnerable	
12.3XA	Vulnerable; contact TAC	
12.3XB	Vulnerable; migrate to 12.3(11)T10 or later	
12.3XC	Vulnerable; contact TAC	
12.3XD	Vulnerable; migrate to 12.3(11)T10 or later	

12.3XE	Vulnerable; contact TAC	
12.3XF	Vulnerable; migrate to 12.3(11)T10 or later	
12.3XG	Vulnerable; contact TAC	
12.3XH	Vulnerable; migrate to 12.3(11)T10 or later	
12.3XI	12.3(7)XI8a	12.3(7)XI9
12.3XJ	Vulnerable; migrate to 12.3(14)YX2 or later	
12.3XK	Vulnerable; migrate to 12.3(14)T7 or later	
12.3XQ	Vulnerable; migrate to 12.4(8) or later	
12.3XR	Vulnerable; contact TAC	
12.3XS	Vulnerable; migrate to 12.4(8) or later	
12.3XU	Vulnerable; migrate to 12.4(2)T4 or later	
12.3XW	Vulnerable; migrate to 12.3(14)YX2 or later	
12.3XX	Vulnerable; migrate to 12.4(8) or later	
12.3XY	Not vulnerable	
12.3YA	Vulnerable; contact TAC	
12.3YD	Vulnerable; migrate to 12.4(2)T4 or later	
12.3YF	Vulnerable; migrate to 12.3(14)YX2 or later	
12.3YG	Vulnerable; migrate to 12.4(2)T4 or later	
12.3YH	Vulnerable; migrate to 12.4(2)T4 or later	
12.3YI	Vulnerable; migrate to 12.4(2)T4 or later	
12.3YJ	Vulnerable; migrate to 12.4(6)T1 or later	
12.3YK	Vulnerable; migrate to 12.4(4)T2 or later	
12.3YM	12.3(14)YM8	
12.3YQ	Vulnerable; migrate to 12.4(6)T1 or later	
12.3YS	Vulnerable; migrate to 12.4(4)T2 or later	
12.3YT	Vulnerable; migrate to 12.4(4)T2 or later	
12.3YU	Vulnerable; migrate to	

	12.4(2)XB2 or later	
12.3YX	12.3(14)YX2	
12.3YZ	12.3(11)YZ1	
Affected 12.4-Based Releases	**Rebuild**	**Maintenance**
12.4	12.4(3d)	
	12.4(5b)	
	12.4(7a)	12.4(8)
12.4MR	Not vulnerable	
12.4SW	All 12.4SW releases are fixed	
12.4T	12.4(2)T4	
	12.4(4)T2	
	12.4(6)T1	12.4(9)T
12.4XA	Vulnerable; migrate to 12.4(6)T1 or later	
12.4XB	12.4(2)XB2	
12.4XC	12.4(4)XC5	
12.4XD	12.4(4)XD2	
12.4XE	All 12.4XE releases are fixed	
12.4XG	All 12.4XG releases are fixed	
12.4XJ	All 12.4XJ releases are fixed	
12.4XP	All 12.4XP releases are fixed	
12.4XT	All 12.4XT releases are fixed	

Top of the section Close Section

回避策

回避策は Type 0 Routing ヘッダを含むパケットをフィルタすることで実現されます。その際には Mobile IPv6 の実装に影響を出さないために、Type 2 Routing ヘッダを含むパケットをフィルタしないように注意する必要があります。どの Cisco IOS ソフトウェアを使用しているか、そして Mobile IPv6 は実装されているかどうかによって以下の回避策を選択することができます。本脆弱性による問題はどのパケット タイプでも発生させることが可能であるため、偽装パケットに対する回避策を適用する際には十分な注意が必要です。

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Mitigation Bulletin』にて参照できます。
http://www.cisco.com/warp/public/707/cisco-amb-20070124-IOS-IPv6.shtml

Mobile IPv6 が導入されていない場合

12.3(4)T よりも前の IOS リリースにおいては、Routing ヘッダを含む全てのパケットをフィルタする必要があります。この方法では Type 0 と Type 2 の Routing ヘッダの区別はつかず、Mobile IPv6 が導入されていない場合のみに有効な回避策となります。

以下に ACL の設定例を示します。

```
Router(config)#ipv6 access-list deny-sourcerouted
Router(config-ipv6-acl)#deny ipv6 any <myaddress1> routing
```

```
Router(config-ipv6-acl)#deny ipv6 any <myaddress2> routing
Router(config-ipv6-acl)#permit ipv6 any any

Router(config-ipv6-acl)#exit
Router(config)#interface Ethernet0
Router(config-if)#ipv6 traffic-filter deny-sourcerouted in
```

この例では、**<myaddressX>** の部分が IPv6 アドレスです。アドレスの例としては、**3ffe:ffff::/64** のようなものがあげられます。ACL は IPv6 が設定されている全てのインターフェイス上に適用される必要があります。もし複数の IPv6 アドレスが 1 つのインターフェイス上に設定されている場合は、それらが全て ACL でカバーされている必要があります。これには、各インターフェイスのすべてのループバック アドレスとリンク ローカル アドレスが含まれます。

全ての IPv6 アドレスを列挙する代替案は、 **deny ipv6 any any routing** を使用することです。ACL を単純化した結果として、Type 0 及び Type 2 Routing ヘッダを持つ全ての IPv6 の通過パケットをフィルタします。設定されている全ての IPv6 アドレスを列挙すれば、通過パケットに対する影響はありません。これは本アドバイサリの全ての例に当てはまります。

Mobile IPv6 が導入されている場合

12.2(15)T よりも前の Cisco IOS リリースを稼働させている場合、回避策はありません。
12.2(15)T 以降の IOS リリースでは、新しいコマンドとして **ipv6 source-route** がサポートされています。このコマンドの適用により、Type 0 の Routing ヘッダを持つ IPv6 パケットをブロックします。設定例を次に示します。

```
Router(config)#no ipv6 source-route
```

これはグローバル コマンドであり、すべてのインターフェイスに適用されます。このコマンドはリンク ローカルやループバックを含む全ての設定されている IPv6 アドレスに対して適用されます。

12.4(2)T 以降の IOS においては、**routing-type** という新しいキーワードが IPv6 ACL 内で指定可能になっています。この指定により特定のルーティング タイプのパケットを選択的に許可または禁止することができます。

```
Router(config)#ipv6 access-list deny-sourcerouted

Router(config-ipv6-acl)#deny ipv6 any <myaddress1> routing-type 0
Router(config-ipv6-acl)#permit ipv6 any any
Router(config)#interface Ethernet0
Router(config-if)#ipv6 source-route
Router(config-if)#ipv6 traffic-filter deny-sourcerouted in
```

このフィルタは IPv6 が設定されている全てのインターフェイスに適用する必要があります。

Top of the section Close Section

修正済みソフトウェアの入手

シスコは本脆弱性の影響を受けるお客様のために、本脆弱性対処用の無償のソフトウェアを提供しています。修正済みソフトウェアが入手可能になり次第、このアドバイザリは更新されます。ソフトウェアの導入を行う前にお客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/public/sw-license-agreement.html に記載のシスコのソフトウェア ライセンスの条項、または Cisco.com ダウンロード サイトの http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

Top of the section Close Section

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、シスコのワールドワイド Web サイト上の Software Center からアップグレードを入手することができます。 http://www.cisco.com

Top of the section Close Section

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

Top of the section Close Section

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無料アップグレードの対象であることをご証明いただくために、製品のシリアル番号を用意し、このお知らせの URL をお知らせください。サービス契約をご利用でないお客様に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、 http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml を参照してください。

Top of the section Close Section

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とその公表は確認しておりません。

本脆弱性は、EADS Corporate Research Center の Arnaud Ebalard 氏からシスコに報告されました。追加の発生条件等に関しては、脆弱性の修正段階においてシスコ内部で確認されたものです。

Top of the section Close Section

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して、単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

Top of the section Close Section

情報配信

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。
http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。 しかしながら、前述のメーリング リストもしくはニュースグループに対し 積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報を ご確認いただくことをお勧めいたします。

Top of the section Close Section

更新履歴

1.2	2007-May-04	**no ipv6 source-rout** affects only Type 0 Routing Header.

1.1	2007-January-27	Updated Cisco IOS software table.
1.0	2007-January-24	Initial public release.

Top of the section Close Section

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは http://www.cisco.com/go/psirt/ で確認することができます。

Top of the section Close Section