Cisco IOS Next Hop Resolution Protocol の脆弱性

High

アドバイザリーID : cisco-sa-20070808-nhrp
初公開日 : 2007-08-08 16:00
バージョン 1.2 : Final
CVSSスコア : 8.0
回避策 : No Workarounds available
Cisco バグ ID : CSCin95836

CVE-2007-4286

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 の Cisco Next Hop Resolution Protocol（NHRP）機能には、デバイスが再起動される可能性のある、またはリモートからコードを実行できるようになる可能性のある、脆弱性が含まれます。

NHRP は、Dynamic Multipoint Virtual Private Network（DMVPN; ダイナミック マルチポイント バーチャル プライベート ネットワーク（VPN））機能の主要コンポーネントです。

NHRP は、3 種類の方法、 つまりリンク層（レイヤ 2）で、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルおよび multipoint GRE（mGRE; マルチポイント GRE）トンネル経由で、または IP（IP プロトコル番号 54）で直接的に動作できます。 この脆弱性は、これら 3 つの動作方法すべてに該当します。

Cisco IOS では、NHRP はデフォルトで有効になっていません。

この脆弱性は、12.2 メインライン以外のリリースに関しては Cisco Bug ID CSCin95836（登録ユーザ専用）に、12.2 メインライン リリースに関しては CSCsi23231（登録ユーザ専用）に記載されています。

このアドバイザリは 808-nhrp で掲示されます。

注: 2007 年 8 月 8 日に公開された情報には、4 つのセキュリティ アドバイザリと 1 つのセキュリティ レスポンスが含まれます。 それらのアドバイザリはすべて IOS に該当し、さらに 1 つは Cisco Unified Communications にも該当します。 各アドバイザリには、そのアドバイザリで説明されている脆弱性を修正したリリースが掲載されているだけでなく、4 つのアドバイザリで説明

されているすべての脆弱性を修正したリリースに関する詳細も掲載されています。 各ドキュメントへのリンクは次のとおりです。

- IPv6 ルーティング ヘッダー使用による Cisco IOS の情報漏えい
  Pv6-leak
- Cisco IOS Next Hop Resolution Protocol の脆弱性
  808-nhrp
- Cisco IOS Secure Copy における認可バイパスの脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-scp
- Cisco IOS および Cisco Unified Communications Manager での音声の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice
- Cisco Unified MeetingPlace XSS の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070808-mp

該当製品

脆弱性のある製品

NHRP 機能を使用するように設定されている IOS が稼働している Cisco デバイスが該当します。 NHRP は、DMVPN 機能との組み合せでも使用されます。

該当するデバイスの実行コンフィギュレーションには、次のコマンドが含まれる場合があります。

```
ip nhrp network-id <ID>
```

このコマンドを設定した後は、実行コンフィギュレーションからこのコマンドを削除するだけでは、NHRP サービスを無効にするのに十分ではありません。 次のコマンドの出力を調べることで、NHRP プロセスが有効かどうかを確認できます。

```
router#show processes | include NHRP
  42 Mwe   F8B8CC           24         76     315 7836/12000   0 NHRP
```

このコマンドで NHRP プロセスが表示される場合は、IOS デバイスで NHRP が実行されています。

NHRP を設定していないのにプロセス テーブルにこのプロセスが表示される場合は、次の作業を行うことでプロセスが表示されないようにできます。

NHRP がデバイスのスタートアップ コンフィギュレーションで設定されていないことを確認し、デバイスをリロードします。 設定から NHRP を削除してデバイスを再起動すると、

NHRP プロセスは実行されなくなります。

脆弱性を含んでいないことが確認された製品

- Cisco IOS が稼働していない Cisco デバイスは該当しません。
- Cisco IOS XR が稼働している Cisco デバイスは該当しません。

これらの脆弱性に該当するその他の Cisco デバイスは現在のところ見つかっていません。

詳細

NHRP は、Nonbroadcast Multiaccess（NBMA; 非ブロードキャスト マルチアクセス）ネットワークでレイヤ 2 からレイヤ 3 への解決を行うことを目的とした、標準ベースのプロトコルです。

ネットワーク デバイスは、NHRP を使用することで、NBMA ネットワークに接続されている他のデバイスのアドレスを検出できます。

NHRP に関する詳細については、
http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_cfg_nhrp_ps6441_TSD_Products_Configuration_Guide_Chapter.html を参照して下さい

NHRP はオープン規格であり、公式の RFC は次の場所にあります。

http://www.rfc-editor.org/rfc/rfc2332.txt

NHRP は、DMVPN で広範に使用され、GRE および mGRE トンネルにおいて搬送でき、IP プロトコル番号 54 として IP データグラム内で直接伝送できます。

GRE または mGRE トンネル経由での NHRP パケットの送信、または IP データグラムでの NHRP としての直接送信から、ルータを保護するための回避策があります。

レイヤ 2 NHRP パケットをブロックするための回避策はありません。 ただし、レイヤ 2 NHRP パケットはルーティング可能ではなく、レイヤ 2 隣接デバイスによって送信される必要があります。

この脆弱性は、2 つの異なる Bug ID によって対応されていました。 Cisco IOS のリリースでこの脆弱性に対処するには、どちらか一方の不具合修正を組み込むだけで十分です。 対応する Bug ID は、12.2 メインライン以外のリリースに関しては CSCin95836（登録ユーザ専用）で、12.2 メインライン リリースに関しては CSCsi23231（登録ユーザ専用）です。

回避策

NHRP 機能が必要ない場合は、NHRP サービスを無効にすることで、この脆弱性による問題の発生を防ぐことができます。

NHRP 機能が必要な場合は、このセクションで示す回避策が影響の軽減に役立ちます。

NHRP が必要な場合、この問題に対する唯一の完全な解決策は、修正済みバージョンのソフトウェアにアップグレードすることです。

ネットワーク内の Cisco デバイスに導入できる追加の緩和策については、このアドバイザリに関連する Cisco 適用対応策速報を次のリンクから参照してください。

808-nhrp

この攻撃はスプーフィングされた送信元アドレスから送信される場合があるので、このセクションの対応策を最も効果的にするには、アンチスプーフィング技法を使用する必要があります。

インフラストラクチャ ACL

ネットワークを移動するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。 インフラストラクチャ ACL はネットワーク セキュリティのベスト プラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワーク セキュリティへの長期的な付加機能として考慮する必要があります。 次の例に示すような ACL を、インフラストラクチャ IP アドレス範囲内の IP アドレスを持つすべてのデバイスを保護するインフラストラクチャ アクセス リストの一部として含める必要があります。

```
router#show processes | include NHRP

  42 Mwe    F8B8CC           24         76     315 7836/12000   0 NHRP
```

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 White Paper は、Web 上の次の場所にあります。

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

コントロール プレーン ポリシング

Control Plane Policing (CoPP; コントロール プレーン ポリシング) を使用すると、信頼できない NHRP (IP プロトコル番号 54) および GRE (IP プロトコル番号 47) から該当デバイスへのアクセスをブロックできます。 Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T は、CoPP 機能をサポートしています。 管理者は、管理プレーンおよびコントロール プレーンを保護するように、デバイスの CoPP を設定できます。 CoPP を設定すると、既存のセキュリティ ポリシーおよび設定に従って、インフラストラクチャ デバイスに送信される承認されたトラフィックだけを明示的に許可することで、インフラストラクチャの直接攻撃のリスクと効果を最小限にすることができます。 次に例を示します。

```
router#show processes | include NHRP

  42 Mwe   F8B8CC           24         76     315 7836/12000   0 NHRP
```

上の CoPP の例では、悪用の可能性のあるパケットと一致する「許可」アクションの Access Control List Entry（ACE; アクセス コントロール リスト エントリ）は policy-map の「drop」機能によってそのパケットを廃棄し、「拒否」アクション（示されていいません）と一致するパケットは policy-map drop 機能には該当しません。 12.2S および 12.0S の Cisco IOS ソフトウェア トレインでは、ポリシーマップの構文が異なることに注意してください。


```
router#show processes | include NHRP

  42 Mwe   F8B8CC           24         76     315 7836/12000   0 NHRP
```


CoPP 機能の設定と使用方法についての詳細は、次のドキュメントを参照してください。

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

および

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.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。

Cisco IOS のビルド方法、番号付け方法、管理方法についての詳細は、次の URL を参照してください。 http://www.cisco.com/warp/public/620/1.html。

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	First Fixed Release (修正された最初のリリース)	推奨リリース
12.0	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0DA	脆弱性なし	
12.0DB	脆弱性なし	
12.0DC	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.0S	12.0(32)S8; 利用可能 な 21-Aug-07	12.0(32)S8; 利用可能 な 21-Aug-07
12.0SC	脆弱性あり; first fixed in 12.3(17a)BC	12.3(17b)BC8 12.3(21a)BC3
12.0SL	脆弱性あり; first fixed in 12.0(32)S8; 利用可能 な 21-Aug-07	12.0(32)S8; 利用可能 な 21-Aug-07
12.0SP	脆弱性あり; first fixed in 12.0(32)S8 利用可能 な 21-Aug-07	12.0(32)S8; 利用可能 な 21-Aug-07
12.0ST	脆弱性あり; first fixed in 12.0(32)S8; 利用可能 な 21-Aug-07	12.0(32)S8; 利用可能 な 21-Aug-07
12.0SX	脆弱性あり; first fixed in 12.0(32)S8; 利用可能 な 21-Aug-07	12.0(32)S8; 利用可能 な 21-Aug-07
12.0SY	12.0(32)SY4; 利用可能 な 21-Aug-07	12.0(32)SY4; 利用可能 な 21-Aug-07
12.0SZ	脆弱性あり; first fixed in 12.0(32)S8; 利用可能 な 21-Aug-07	
12.0T	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0W	脆弱性なし	
12.0WC	脆弱性なし	
12.0WT	脆弱性なし	
12.0XA	脆弱性あり; first fixed in	12.2(46a)

	12.2(46)	
12.0XB	脆弱性なし	
12.0XC	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XD	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XE	脆弱性あり; first fixed in 12.1(27b)E3; 利用可能 な 10-Aug-07	
12.0XF	脆弱性なし	
12.0XG	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XH	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XI	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XJ	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XK	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XL	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XM	脆弱性なし	
12.0XN	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XQ	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XR	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.0XS	脆弱性なし	
12.0XV	脆弱性なし	
12.0XW	脆弱性なし	
該当する 12.1 ベースのリリース	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.1	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1AA	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1AX	脆弱性なし	
12.1AY	脆弱性なし	
12.1AZ	脆弱性なし	
12.1CX	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1DA	12.2(10)DA8 12.2(12)DA12	12.2(10)DA8 12.2(12)DA12

12.1DB	脆弱性なし	
12.1DC	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.1E	12.1(27b)E3; 利用可能 な 5-Mar-08	
12.1EA	脆弱性なし	
12.1EB	脆弱性なし	
12.1EC	脆弱性あり; first fixed in 12.3(17a)BC	12.3(17b)BC8 12.3(21a)BC3
12.1EO	脆弱性なし	
12.1EU	脆弱性あり; first fixed in 12.2(25)EWA10	12.2(25)EWA 10
12.1EV	脆弱性なし	
12.1EW	脆弱性あり; first fixed in 12.2(25)EWA10	すべての Cat4K プラットフォーム： 12.2(25)EWA 10 12.2(31)SGA3 12.2(37)SG1 12.2(40)SG; 利用可能 な Oct-07
12.1EX	脆弱性あり; first fixed in 12.1(27b)E3; 利用可能 な 5-Mar-08	
12.1EY	脆弱性なし	
12.1EZ	脆弱性あり; first fixed in 12.1(27b)E3; 利用可能 な 5-Mar-08	
12.1GA	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1GB	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1T	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XA	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XB	脆弱性なし	
12.1XC	脆弱性あり; first fixed in	12.2(46a)

	12.2(46)	
12.1XD	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XE	脆弱性なし	
12.1XF	脆弱性なし	
12.1XG	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XH	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XI	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XJ	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XK	脆弱性なし	
12.1XL	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XM	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-

		Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XN	脆弱性なし	
12.1XO	脆弱性なし	
12.1XP	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XQ	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XR	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XS	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XT	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-

		Aug-07
12.1XU	脆弱性なし	
12.1XV	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XW	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XX	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XY	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1XZ	脆弱性あり; first fixed in 12.2(46)	12.2(46a)
12.1YA	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YB	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YC	脆弱性なし	
12.1YD	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利

		用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YE	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YF	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YG	脆弱性なし	
12.1YH	脆弱性なし	
12.1YI	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YJ	脆弱性なし	
該当する 12.2 ベースのリリース	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.2	12.2(26c); 利用可能 な 14-Aug-07 12.2(27c); 利用可能 な 14-Aug-07 12.2(28d); 利用可能 な 14-Aug-07 12.2(29b); 利用可能 な 14-	12.2(46a)

	Aug-07 12.2(46)	
12.2B	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2BC	脆弱性あり; first fixed in 12.3(17a)BC	12.3(17b)BC8 12.3(21a)BC3
12.2BW	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2BY	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2BZ	脆弱性あり; first fixed in 12.3(7)XI10a 利用可能 な 21-Aug-07	12.3(7)XI10a; 利用可能 な 21-Aug-07
12.2CX	脆弱性あり; first fixed in 12.3(17a)BC	12.3(17b)BC8 12.3(21a)BC3
12.2CY	脆弱性あり; first fixed in 12.3(17a)BC	12.3(17b)BC8 12.3(21a)BC3
12.2CZ	脆弱性なし	
12.2DA	12.2(10)DA8 12.2(12)DA12	12.2(10)DA8 12.2(12)DA12
12.2DD	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-

		Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2DX	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2EU	脆弱性あり; first fixed in 12.2(25)EWA10	すべての Cat4K プラットフォーム：12.2(25)EWA 10 12.2(31)SGA3 12.2(37)SG1 12.2(40)SG; 利用可能 な Oct-07
12.2EW	脆弱性あり; first fixed in 12.2(25)EWA10	すべての Cat4K プラットフォーム：12.2(25)EWA 10 12.2(31)SGA3 12.2(37)SG1 12.2(40)SG; 利用可能 な Oct-07
12.2EWA	12.2(25)EWA10	すべての Cat4K プラットフォーム：12.2(25)EWA 10 12.2(31)SGA3 12.2(37)SG1 12.2(40)SG; 利用可能 な Oct-07
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	
12.2IXA	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	
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性あり; first fixed in 12.2(25)SW11	12.2(25)SW11
12.2MC	12.2(15)MC2h 12.2(15)MC2j	12.2(15)MC2j
12.2S	12.2(14)S19 12.2(18)S13 12.2(20)S14 12.2(25)S13	12.2(25)S13 12.2(14)S19
12.2SB	12.2(28)SB9 12.2(31)SB6	12.2(28)SB9; 利用可能 な 15-Aug-07 12.2(31)SB6
12.2SBC	脆弱性あり; first fixed in 12.2(31)SB6	12.2(28)SB9; 利用可能 な 15-Aug-07 12.2(31)SB6
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	12.2(25)SG2; 利用可能 な 13-Aug-07 12.2(31)SG2; 利用可能 な 13-Aug-07 12.2(37)SG1; 利用可能 な 13-Aug-07 12.2(40)SG; 利用可能 な 24-Oct-07	すべての Cat4K プラットフォーム： 12.2(25)SG2 12.2(37)SG1 12.2(31)SG2 12.2(40)SG; 利用可能 な Oct-07
12.2SGA	12.2(31)SGA3 12.2(31)SGA4; 利用可能 な 15-Oct-07	すべての Cat4K プラットフォーム： 12.2(31)SGA3 12.2(37)SG1 12.2(40)SG;

		利用可能 な Oct-07
12.2SL	脆弱性なし	
12.2SM	12.2(29)SM2; 利用可能 な 22-Aug-07	12.2(29)SM2; 利用可能 な 10-Aug-07
12.2SO	脆弱性なし	
12.2SRA	脆弱性なし	
12.2SRB	脆弱性なし	
12.2SU	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2SV	12.2(29)SV4; 利用可能 な 14-Oct-07	12.2(29)SV4; 利用可能 な 14-Oct-07
12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	
12.2SW	12.2(25)SW11	12.2(25)SW11
12.2SX	脆弱性あり; first fixed in 12.2(18)SXE4	
12.2SXA	脆弱性あり; first fixed in 12.2(18)SXE4	
12.2SXB	脆弱性あり; first fixed in 12.2(18)SXE4	12.2(18)SXF10
12.2SXD	脆弱性あり; contact TAC	
12.2SXE	12.2(18)SXE4	12.2(18)SXF10
12.2SXF	脆弱性なし	
12.2SXH	脆弱性なし	
12.2SY	脆弱性あり; first fixed in 12.2(18)SXE4	
12.2SZ	脆弱性あり; first fixed in 12.2(25)S13	12.2(25)S13 12.2(14)S19
12.2T	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07

		12.3(17c); 利用可能な 16-Aug-07
12.2TPC	12.2(8)TPC10c; 利用可能な 17-Aug-07	12.2(8)TPC10c
12.2UZ	脆弱性あり; first fixed in 12.2(31)SB6	12.2(28)SB9; 利用可能な 15-Aug-07 12.2(31)SB6
12.2VZ	脆弱性あり; first fixed in 12.2(31)SB6	12.2(28)SB9; 利用可能な 15-Aug-07 12.2(31)SB6
12.2XA	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能な 16-Aug-07 12.3(17c); 利用可能な 16-Aug-07
12.2XB	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能な 16-Aug-07 12.3(17c); 利用可能な 16-Aug-07
12.2XC	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2XD	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利

		用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XE	脆弱性なし	
12.2XF	脆弱性あり; first fixed in 12.3(17a)BC	12.3(17b)BC8 12.3(21a)BC3
12.2XG	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XH	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XI	脆弱性なし	
12.2XJ	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XK	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利

		用可能 な 16-Aug-07
12.2XL	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XM	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XN	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XQ	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XR	12.3(2)JA3	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利

		用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XS	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XT	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XU	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XV	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XW	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b)

		12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YA	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YB	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YC	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YD	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YE	脆弱性あり; first fixed in	12.2(25)S13

	12.2(25)S13	12.2(14)S19
12.2YF	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YG	脆弱性なし	
12.2YH	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YJ	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YK	脆弱性なし	
12.2YL	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YM	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-

		Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YN	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YO	脆弱性なし	
12.2YP	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YQ	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YR	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YS	脆弱性なし	
12.2YT	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b)

		12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YU	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YV	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YW	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YX	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YY	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用

		可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YZ	脆弱性あり; first fixed in 12.2(25)S13	12.2(25)S13 12.2(14)S19
12.2ZA	脆弱性あり; first fixed in 12.2(18)SXE4	
12.2ZB	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZC	脆弱性なし	
12.2ZD	脆弱性あり; contact TAC	
12.2ZE	脆弱性あり; first fixed in 12.3(17a)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2ZF	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZG	脆弱性あり; contact TAC	12.3(2)XA6 12.3(8)YG6; 利用可能 な 16-Aug-07
12.2ZH	脆弱性あり; contact TAC	12.2(13)ZH9
12.2ZJ	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h)

		12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZL	脆弱、Cisco 17xx のための first fixed in 12.3(14)T5; Cisco 3200 については 12.4(1c) で初めて修正 12.3(7)XR7 で初めて修正 （ICS7750 用は 2007 年 8 月 13 日に入手可能）	
12.2ZP	脆弱性なし	
12.2ZR	脆弱性あり; contact TAC	
12.2ZU	脆弱性なし	
12.2ZW	脆弱性なし	
12.2ZY	脆弱性なし	
該当する 12.3 ベースのリリース	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.3	12.3(17a) 12.3(18) 12.3(19) 12.3(20) 12.3(21) 12.3(22) 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.3B	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3BC	12.3(17a)BC 12.3(21)BC	12.3(17b)BC8 12.3(21a)BC3
12.3BW	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用

		可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
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	
12.3JK	脆弱性なし	
12.3JL	脆弱性なし	
12.3JX	脆弱性なし	
12.3T	一部のプラットフォームをサポート 12.3(11)T12; 利用可能 な 16-Aug-07 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3TPC	12.3(4)TPC11b; 利用可能 な 17-Aug-07	12.3(4)TPC11b; 利用可能 な 17-Aug-07
12.3VA	脆弱性なし	
12.3XA	12.3(2)XA6	12.3(2)XA6
12.3XB	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XC	12.3(2)XC5	12.3(2)XC5
12.3XD	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)

12.3XE	12.3(2)XE5; 利用可能 な 17-Aug-07	12.3(2)XE5
12.3XF	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XG	脆弱性あり; contact TAC	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XH	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XI	12.3(7)XI10a; 利用可能 な 21-Aug-07	12.3(7)XI10a; 利用可能 な 21-Aug-07
12.3XJ	脆弱性あり; first fixed in 12.3(14)YX8	12.3(14)YX9; 利用可能 な 13-Aug-07
12.3XK	脆弱性あり; first fixed in 12.3(14)T5	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XQ	脆弱性あり; first fixed in 12.4(1c)	12.4(12c) 12.4(3h) 12.4(5c)

		12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XR	12.3(7)XR7; 利用可能 な 17-Aug-07	12.3(7)XR7; 利用可能 な 17-Aug-07
12.3XS	脆弱性あり; first fixed in 12.4(1c)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XU	脆弱性あり; first fixed in 12.4(4)T	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3XW	脆弱性あり; first fixed in 12.3(14)YX8	12.3(14)YX9; 利用可能 な 13-Aug-07
12.3XY	脆弱性なし	
12.3YA	脆弱性あり; first fixed in 12.4(1c)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d) 12.3(8)YG6; 利用可能 な 16-Aug-07
12.3YD	脆弱性あり; first fixed in 12.4(4)T	12.4(11)T3 12.4(9)T5; 利

		用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YF	脆弱性あり; first fixed in 12.3(14)YX8	12.3(14)YX9; 利用可能 な 13-Aug-07
12.3YG	12.3(8)YG6; 利用可能 な 16-Aug-07	12.3(8)YG6; 利用可能 な 16-Aug-07
12.3YH	脆弱性あり; first fixed in 12.4(4)T	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YI	脆弱性あり; first fixed in 12.4(4)T	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YJ	脆弱性あり; first fixed in 12.4(4)T	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1

12.3YK	12.3(11)YK3; 利用可能 な 20-Aug-07	12.3(11)YK3; 利用可能 な 20-Aug-07
12.3YM	12.3(14)YM5	12.3(14)YM11; 利用可能 な 23-Aug-07
12.3YQ	脆弱性あり; first fixed in 12.4(4)T	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YS	12.3(11)YS2; 利用可能 な 17-Aug-07	12.3(11)YS2
12.3YT	脆弱性あり; first fixed in 12.4(4)T	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YU	脆弱性あり; first fixed in 12.4(2)XB6 利用可能 な 16-Aug-07	12.4(2)XB6; 利用可能 な 16-Aug-07
12.3YX	12.3(14)YX8	12.3(14)YX9; 利用可能 な 13-Aug-07
12.3YZ	12.3(11)YZ2; 利用可能 な 17-Aug-07	12.3(11)YZ2; 利用可能 な 17-Aug-07
該当する 12.4 ベースのリリース	**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(1c) 12.4(10) 12.4(12) 12.4(13) 12.4(16) 12.4(3b) 12.4(5)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f)

	12.4(7) 12.4(8)	12.4(16) 12.4(10c) 12.4(13d)
12.4JA	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	12.4(12)MR1 12.4(11)MR 12.4(12)MR 12.4(12)MR2; 利用可能 な 14-Aug-07 12.4(4)MR 12.4(6)MR 12.4(9)MR	12.4(12)MR2
12.4SW	脆弱性なし	
12.4T	12.4(11)T 12.4(15)T 12.4(2)T3 12.4(4)T 12.4(6)T 12.4(9)T	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.4XA	脆弱性なし	
12.4XB	12.4(2)XB6; 利用可能 な 16-Aug-07	12.4(2)XB6; 利用可能 な 16-Aug-07
12.4XC	脆弱性なし	
12.4XD	脆弱性なし	
12.4XE	脆弱性なし	
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性なし	
12.4XK	脆弱性なし	
12.4XT	脆弱性なし	
12.4XV	脆弱性なし	
12.4XW	脆弱性なし	

不正利用事例と公式発表

この問題が悪用された例は報告されておらず、悪用コードは研究者によってパブリック メーリング リストで公開されています。

この脆弱性は、Martin Kluge から Cisco に報告されたものです。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-nhrp

改訂履歴

リビジョン 1.2	2008-April-25	CSCin95836 および CSCin23231 のための CVSS スコアへの 更新済リンク 。
リビジョン 1.1	2007 年 8 月 9 日	「不正利用と公表」セクションの公開悪用コード情報をアップデート。
リビジョン 1.0	2007 年 8 月 8 日	初回公開リリース

利用規約