Cisco IOS および Cisco IOS-XR で IPv6 ルーティング ヘッダーを使用した場合の情報漏えい

High

アドバイザリーID : cisco-sa-20070808-IOS-IPv6-leak

初公開日 : 2007-08-08 16:00

バージョン 1.1 : Final

CVSSスコア : 8.0

回避策 : No Workarounds available

Cisco バグ ID : CSCef77013

CVE-2007-4285

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 および Cisco IOS XR には、Type 0 ルーティング ヘッダーが存在する特別に作成された IPv6 パケットの処理に関して脆弱性があります。 この脆弱性が悪用されると、該当する IOS および IOS XR デバイスで情報が漏えいする場合があり、さらに IOS デバイスがクラッシュする可能性もあります。 Cisco IOS XR デバイスを実行するデバイスでこの脆弱性が悪用されると、デバイス自体はクラッシュしませんが、IPv6 サブシステムがクラッシュする可能性があります。

シスコでは、該当するお客様用に、この脆弱性に対応する無償ソフトウェアを提供しております。 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。

このアドバイザリは Pv6-leak 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

この脆弱性が該当するのは、IPv6 プロトコルを使用するように設定されていて、次のいずれかの種類のソフトウェアの該当バージョンが稼働しているデバイスです。

- Cisco IOS
- Cisco IOS XR

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。 出力の次の行には、カッコに囲まれたイメージ名が表示され、その後にバージョンと Cisco IOS リリース名が続きます。 その他の Cisco 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。

次の例は、IOS イメージを実行しているデバイスからの出力例です。

```
Router>show version
Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(14)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 31-Mar-05 08:04 by yiyan
```

Cisco IOS ソフトウェア リリースの命名方法に関する詳細については、次のリンクを参照してください。 http://www.cisco.com/warp/public/620/1.html。

IOS デバイスで IPv6 が設定されているかどうかを調べるには、次の例に示すように、Cisco IOS の設定で **ipv6** を含む行を確認してください。

```
Router#show running-config | include ipv6
ipv6 address 2001:0DB8:C18:1::/64 eui-64
```

設定にこの例のような行が含まれる場合、そのデバイスでは IPv6 が設定されています。 厳密な IPv6 アドレスは設定によって異なります。

IOS XR デバイスで IPv6 が設定されているかどうかを調べるには、Cisco IOS XR の設定に次の行が含まれているかどうかを確認します。

```
Router-IOS_XR#show ipv6 interface | include IPv6
IPv6 is enabled, link-local address is fe80::216:47ff:fee1:d987
IPv6 is disabled, link-local address unassigned
IPv6 is disabled, link-local address unassigned
```

出力の少なくとも 1 つの行に **IPv6 is enabled** という表記が含まれる場合、そのデバイスには IPv6 が設定されています。

脆弱性を含んでいないことが確認された製品

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。特に、次のデバイスは該当しないことが確認されています。

- Cisco PIX および ASA アプライアンス
- Cisco Firewall Services Module（FWSM）
- Cisco MDS

Cisco PIX、ASA、および FWSM ファイアウォール製品は、IPv6 ルーティング ヘッダーを含むパケットを処理しません。 そのようなパケットはすべて廃棄されます。

詳細

このドキュメントで説明されている脆弱性が悪用されると、IPv6 パケット ヘッダーの宛先 IPv6 アドレスとパケット バッファ メモリの 16 バイトの間で、メモリのスワップが発生する可能性があります。 この脆弱性によってアクセス可能なメモリは、パケット ヘッダーの先頭から 1500 バイトまでです。

この脆弱性は、Cisco IOS については Cisco Bug ID CSCef77013（登録ユーザ専用）に、Cisco IOS XR については Cisco Bug ID CSCsi74127（登録 ユーザ専用）に記載されています。

脆弱性スコア評価の詳細

Cisco では、Common Vulnerability Scoring System（CVSS）に基づき、このアドバイザリで説明されている脆弱性のスコアを評価しました。 このセキュリティ アドバイザリの CVSS スコア評価は、CVSS バージョン 1.0 に従って行われました。

Cisco では基本スコアと現状スコアを評価します。 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、すべてのケースにおける重みを「標準」に設定します。 特定の脆弱性の環境的影響を判断する際には、重みパラメータを適用することを推奨します。

CVSS は、脆弱性の重大度を伝える標準ベースのスコア評価方式であり、対応の緊急度や優先度を判断するのに役立ちます。

Cisco は http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html で CVSS に関する追加質問に答えるために FAQ を提供しました。

Cisco はまた http://tools.cisco.com/security/center/cvssCalculator.x で個々 の ネットワークのための環境影響の計算を助けるように CVSS カルキュレータを提供しました。

CSCef77013：Tighter parameter checking for IPv6（登録ユーザ専用） CSCef77013 の環境スコアを計算する						
CVSS 基本スコア：8						
攻撃元区分	攻撃条件の複雑さ	認証	機密性への影響	完全性への影響	可用性への影響	影響の重み
Remote	低	不要	部分的	部分的	Complete	Normal
現状スコア - 6.6						
攻撃される可能性		利用可能な対策のレベル		Report Confidence		
機能する		正式		確認済		

CSCsi74127：Processing of IPv6 headers（登録ユーザ専用） CSCsi74127 の環境スコアを計算する						
CVSS 基本スコア：7						
攻撃元区分	攻撃条件の複雑さ	認証	機密性への影響	完全性への影響	可用性への影響	影響の重み
Remote	低	不要	部分的	部分的	部分的	Normal
現状スコア - 5.8						
攻撃される可能性		利用可能な対策のレベル		Report Confidence		
機能する		正式		確認済		

回避策

Type 0 ルーティング ヘッダーを含むパケットをフィルタリングすることが回避策となります。タイプ 2 ルーティング ヘッダーを含むパケットをフィルタリングしないよう、十分に注意する必要があります。このパケットをフィルタリングすると、モバイル IPv6 の展開に支障が生じます。使用している Cisco IOS ソフトウェアのリリースによっては、モバイル IPv6 が展開されている場合、複数の回避策が存在する可能性があります。 この脆弱性を悪用する際には任意のパケットタイプ（TCP、UDP、ICMP）を使用できるので、スプーフィングされた IPv6 パケットに対して回避策を適用する場合は、注意する必要があります。

Cisco IOS XR を実行し、モバイル IPv6 が展開されているデバイスの場合、回避策はありません

。

IPv6 ルーティング ヘッダーに対する保護メカニズムについての詳細は、次の場所にある Applied Intelligence White Paper『IPv6 タイプ 0 ルーティング ヘッダーの悪用に対する対応策』を参照してください。

http://www.cisco.com/web/about/security/intelligence/countermeasures-for-ipv6-type0-rh.html。

Cisco IOS を実行しているデバイス

コントロール プレーン ポリシング

次の例は、モバイル IPv6 が展開されているかどうかに関係なく適用できます。

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、該当デバイスに対する、Type 0 ルーティング ヘッダーを含む信頼できない IPv6 パケット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。 デバイスに CoPP を設定して、管理プレーンとコントロール プレーンを保護し、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の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への直接攻撃のリスクと効果を最小限に抑えることができます。 次の例をネットワークに適用できます。

```
Router-IOS_XR#show ipv6 interface | include IPv6
IPv6 is enabled, link-local address is fe80::216:47ff:fee1:d987
IPv6 is disabled, link-local address unassigned
IPv6 is disabled, link-local address unassigned
```

上の CoPP の例には、悪用の可能性が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）があるので、policy-map の「drop」機能によってこれらのパケットは廃棄されます。

CoPP 機能の設定および使用のその他の情報は 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 で見つけることができます。

モバイル IPv6 が展開されていない場合

12.2(15)T より古いリリースの IOS に適用できる回避策は、ACL を使用してルーティング ヘッダーを含むすべてのパケットをフィルタリングすることです。 この方法は、Type 0 と Type 2 のルーティング ヘッダーを区別できないので、モバイル IPv6 が展開されている場合には適していません。

次の例は、そのような ACL を設定する方法を示しています。

```
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
```

上の例の <myaddressX> は IPv6 アドレスです。 2001:DB8:900D::1/64 はこのようなアドレスの一例です。 ACL は、すべてのインターフェイスに対して適用され、設定されているすべての IPv6 アドレスを含んでいる必要があります。 1 つのインターフェイスに複数の IPv6 アドレスが設定されている場合は、すべてのアドレスを ACL でカバーする必要があります。 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。

すべての IPv6 アドレスを列挙する代わりに、deny ipv6 any any routing ステートメントを使用することもできます。 この方法を使用すると、ACL の内容は簡単になりますが、ルーティング ヘッダー 0 および 2 を含むすべてのトランジット IPv6 トラフィックもフィルタリングされます。 設定されているすべての IPv6 アドレスを列挙した場合、トランジット トラフィックは影響を受けません。 このことは、このアドバイザリの他のすべての例にも当てはまります。

新しいコマンド **ipv6 source-route** が、IOS リリース 12.2(15)T 以降で導入されています。 このコマンドを適用すると、デバイス自体が受信した、Type 0 ルーティング ヘッダーを含むすべての IPv6 パケットが廃棄されます (たとえば、IPv6 宛先アドレスは、デバイスに設定されている任意の IPv6 アドレスと一致します)。 このコマンドは、トランジット トラフィックには適用されません。 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 アドレスやループバック アドレスを含むすべての定義済み IPv6 アドレスおよびすべてのインターフェイスに適用できます。

モバイル IPv6 が展開されている場合

Cisco IOS リリース実行するデバイスのための回避策は 12.2(15)T 以前ありません。 新しいコマンド **ipv6 source-route** が、IOS リリース 12.2(15)T 以降で導入されています。 このコマンドを適用すると、デバイス自体が受信した、Type 0 ルーティング ヘッダーを含むすべての IPv6 パケットが廃棄されます (たとえば、IPv6 宛先アドレスは、デバイスに設定されている任意の IPv6 アドレスと一致します)。 このコマンドは、トランジット トラフィックには適用されません。 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 アドレスやループバック アドレスを含むすべての定義済み IPv6 アドレスおよびすべてのインターフェイスに適用できます。

IOS 12.4(2)T では、新しいキーワード routing-type が IPv6 の ACL に追加されています。 このキーワードを使用すると、特定のルーティング タイプを選択して許可または拒否できます。

```
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 traffic-filter deny-sourcerouted in
```

この IPv6 ACL は、IPv6 アドレスが設定されているすべてのインターフェイスにインバウンドで適用する必要があります。

Cisco IOS XR を実行しているデバイス

モバイル IPv6 が展開されていない場合

ACL を使用してルーティング ヘッダーを含むすべてのパケットをフィルタリングすることが回避策になります。 この方法は、Type 0 と Type 2 のルーティング ヘッダーを区別できないので、モバイル IPv6 が展開されている場合には適していません。

次の例は、そのような ACL を設定する方法を示しています。

```
Router-IOS_XR#configure terminal
Router-IOS_XR(config)#ipv6 access-list deny-ipv6-type0-rh
Router-IOS_XR(config-ipv6-acl)#deny ipv6 any host 2001:0DB8:12::3 routing
Router-IOS_XR(config-ipv6-acl)#permit ipv6 any any
Router-IOS_XR(config-ipv6-acl)#exit
Router-IOS_XR(config)#interface GigabitEthernet 0/0/0/1
Router-IOS_XR(config-if)#ipv6 access-group deny-ipv6-type0-rh ingress
Router-IOS_XR(config-if)#end
```

ACL は、すべてのインターフェイスに対して適用され、設定されているすべての IPv6 アドレスを含んでいる必要があります。 1 つのインターフェイスに複数の IPv6 アドレスが設定されている場合は、すべてのアドレスを ACL で力バーする必要があります。 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。

モバイル IPv6 が展開されている場合

モバイル IPv6 が展開されている場合、回避策はありません。

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	脆弱性なし	
12.0DA	脆弱性なし	
12.0DB	脆弱性なし	
12.0DC	脆弱性なし	
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	脆弱性なし	
12.0SL	脆弱性なし	
12.0SP	脆弱性なし	
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	12.0(32)SY4;

	21-Aug-07	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	脆弱性なし	
12.0W	脆弱性なし	
12.0WC	脆弱性なし	
12.0WT	脆弱性なし	
12.0XA	脆弱性なし	
12.0XB	脆弱性なし	
12.0XC	脆弱性なし	
12.0XD	脆弱性なし	
12.0XE	脆弱性なし	
12.0XF	脆弱性なし	
12.0XG	脆弱性なし	
12.0XH	脆弱性なし	
12.0XI	脆弱性なし	
12.0XJ	脆弱性なし	
12.0XK	脆弱性なし	
12.0XL	脆弱性なし	
12.0XM	脆弱性なし	
12.0XN	脆弱性なし	
12.0XQ	脆弱性なし	
12.0XR	脆弱性なし	
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	脆弱性なし	
12.1AA	脆弱性なし	
12.1AX	脆弱性なし	
12.1AY	脆弱性なし	
12.1AZ	脆弱性なし	
12.1CX	脆弱性なし	
12.1DA	脆弱性なし	
12.1DB	脆弱性なし	
12.1DC	脆弱性なし	
12.1E	脆弱性なし	
12.1EA	脆弱性なし	
12.1EB	脆弱性なし	

12.1EC	脆弱性なし	
12.1EO	脆弱性なし	
12.1EU	脆弱性なし	
12.1EV	脆弱性なし	
12.1EW	脆弱性なし	
12.1EX	脆弱性なし	
12.1EY	脆弱性なし	
12.1EZ	脆弱性なし	
12.1GA	脆弱性なし	
12.1GB	脆弱性なし	
12.1T	脆弱性なし	
12.1XA	脆弱性なし	
12.1XB	脆弱性なし	
12.1XC	脆弱性なし	
12.1XD	脆弱性なし	
12.1XE	脆弱性なし	
12.1XF	脆弱性なし	
12.1XG	脆弱性なし	
12.1XH	脆弱性なし	
12.1XI	脆弱性なし	
12.1XJ	脆弱性なし	
12.1XK	脆弱性なし	
12.1XL	脆弱性なし	
12.1XM	脆弱性なし	
12.1XN	脆弱性なし	
12.1XO	脆弱性なし	
12.1XP	脆弱性なし	
12.1XQ	脆弱性なし	
12.1XR	脆弱性なし	
12.1XS	脆弱性なし	
12.1XT	脆弱性なし	
12.1XU	脆弱性あり; first fixed in 12.3(15)	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
12.1XV	脆弱性あり; first fixed in 12.3(15)	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	脆弱性なし	
12.1XX	脆弱性なし	
12.1XY	脆弱性なし	
12.1XZ	脆弱性なし	
12.1YA	脆弱性なし	
12.1YB	脆弱性あり; first fixed in 12.3(15)	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	脆弱性あり; first fixed in 12.3(15)	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
12.1YD	脆弱性あり; first fixed in 12.3(15)	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	脆弱性なし	
12.1YF	脆弱性なし	
12.1YG	脆弱性なし	
12.1YH	脆弱性なし	

12.1YI	脆弱性なし	
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	脆弱性なし	
12.2B	脆弱性あり; first fixed in 12.3(14)T	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(15)	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)T	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	脆弱性なし	
12.2CX	脆弱性あり; first fixed in 12.3(17a)BC	12.3(17b)BC8 12.3(21a)BC3
12.2CY	脆弱性なし	
12.2CZ	脆弱性なし	
12.2DA	脆弱性なし	
12.2DD	脆弱性あり; first fixed in 12.3(14)T	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)T	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)EWA10 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)EWA10 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)EWA10 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	脆弱性あり; first fixed in	12.2(25)SEE4

	12.2(25)SEE4	; 利用可能 な 07-Aug-07
12.2FX	脆弱性なし	
12.2FY	脆弱性なし	
12.2FZ	脆弱性あり; first fixed in 12.2(35)SE	12.2(40)SE; 利用可能 な 24-Aug-07 12.2(37)SE1 12.2(35)SE5
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	
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性なし	
12.2MC	12.2(15)MC2h 12.2(15)MC2j	12.2(15)MC2j
12.2S	12.2(14)S18 12.2(18)S13 12.2(20)S14 12.2(25)S13 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2SB	脆弱性なし	
12.2SBC	脆弱性なし	
12.2SE	脆弱性なし	
12.2SEA	脆弱性あり; first fixed in 12.2(25)SEE4	12.2(25)SEE4 ; 利用可能 な 07-Aug-07
12.2SEB	脆弱性あり; first fixed in 12.2(25)SEE4	12.2(25)SEE4 ; 利用可能 な 07-Aug-07
12.2SEC	脆弱性あり; first fixed in 12.2(25)SEE4	12.2(25)SEE4 ; 利用可能 な 07-Aug-07
12.2SED	脆弱性あり; first fixed in 12.2(25)SEE4	12.2(25)SEE4 ; 利用可能 な 07-Aug-07
12.2SEE	12.2(25)SEE4	12.2(25)SEE4
12.2SEF	脆弱性なし	
12.2SEG	12.2(25)SEG3	12.2(25)SEG 3
12.2SG	12.2(25)SG2; 利用可能 な 13-Aug-07 12.2(31)SG1 12.2(31)SG 12.2(37)SG	すべての Cat4K プラットフォーム： 12.2(25)SG2 12.2(37)SG1

	12.2(40)SG; 利用可能 な 24-Oct-07	12.2(31)SG2 12.2(40)SG; 利用可能 な Oct-07
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	
12.2SU	脆弱性あり; first fixed in 12.3(14)T	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(27)SV2 12.2(27)SV3 12.2(27)SV1 12.2(28)SV1 12.2(29)SV 12.2(29a)SV 12.2(29b)SV	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)SXE	
12.2SXA	脆弱性あり; first fixed in 12.2(18)SXE	
12.2SXB	脆弱性あり; first fixed in 12.2(18)SXE	12.2(18)SXF10
12.2SXD	脆弱性あり; contact TAC	
12.2SXE	脆弱性なし	
12.2SXF	脆弱性なし	
12.2SXH	脆弱性なし	
12.2SY	脆弱性あり; first fixed in 12.2(18)SXE	
12.2SZ	脆弱性あり; first fixed in 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2T	脆弱性あり; first fixed in 12.3(15)	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	脆弱性なし	
12.2VZ	脆弱性なし	
12.2XA	脆弱性あり; first fixed in 12.3(15)	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(15)	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)T	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(15)	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(15)	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(15)	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	脆弱性あり; first fixed in 12.3(15)	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
12.2XJ	脆弱性あり; first fixed in 12.3(15)	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(15)	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(15)	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(15)	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(15)	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(15)	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	脆弱性なし	
12.2XS	脆弱性なし	
12.2XT	脆弱性あり; first fixed in 12.3(15)	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(15)	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(15)	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(15)	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(15)	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(15)	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	脆弱性なし	
12.2YD	脆弱性あり; first fixed in 12.3(14)T	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(30)S	12.2(25)S13 12.2(14)S19
12.2YF	脆弱性あり; first fixed in 12.3(15)	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(15)	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(15)	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)T	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)T	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)T	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	脆弱性なし	
12.2YQ	脆弱性あり; first fixed in 12.3(14)T	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)T	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(15)	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)T	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)T	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	12.4(12c)

	12.3(14)T	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)T	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)T	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(30)S	12.2(25)S13 12.2(14)S19
12.2ZA	脆弱性あり; first fixed in 12.2(18)SXE	
12.2ZB	脆弱性あり; first fixed in 12.3(14)T	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(15)	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)T	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	脆弱性なし	
12.2ZH	12.2(13)ZH9; 利用可能 な 17-Aug-07	12.2(13)ZH9
12.2ZJ	脆弱性あり; first fixed in 12.3(14)T	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)T; Cisco 3200 については 12.4(1) 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(15) 12.3(16) 12.3(17a) 12.3(18) 12.3(19) 12.3(20) 12.3(21)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-

	12.3(22) 12.3(23)	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)T	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)T	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)
12.3JA	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)T	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	脆弱性なし	
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)T	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)T	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)T	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)T	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)YX	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)T	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(1)	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(1)	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(2)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)YX	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(1)	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(2)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)YX	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(2)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(2)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 12.3(14)YQ	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	脆弱性なし	
12.3YQ	脆弱性なし	
12.3YS	脆弱性なし	
12.3YT	脆弱性なし	
12.3YU	脆弱性なし	
12.3YX	脆弱性なし	
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**
該当する 12.4 ベースのリリースはありません。		

Cisco IOS XR

修正済み Cisco IOS XR ソフトウェアの一覧を次の表に示します。

Cisco IOS XR のバージョン	SMU ID	SMU 名
3.2.3	AA01920	hfr-base-3.2.3.CSCsi74127
3.2.4	AA01919	hfr-base-3.2.4.CSCsi74127
3.2.6	AA01918	hfr-base-3.2.6.CSCsi74127
3.3.0	AA01917	hfr-base-3.3.0.CSCsi74127
3.3.1	AA01916	hfr-base-3.3.1.CSCsi74127
3.3.2	AA01915	hfr-base-3.3.2.CSCsi74127

3.3.3	AA01914	hfr-base-3.3.3.CSCsi74127
3.3.4	AA01913	hfr-base-3.3.4.CSCsi74127
3.4.0	AA01912	hfr-base-3.4.0.CSCsi74127
3.4.1	AA01911	hfr-base-3.4.1.CSCsi74127
3.4.2	AA02124	hfr-base-3.4.2.CSCsi74127
3.3.1	AA01910	c12k-base-3.3.1.CSCsi74127
3.4.0	AA01909	c12k-base-3.4.0.CSCsi74127
3.4.1	AA01908	c12k-base-3.4.1.CSCsi74127

IOS XR パッケージ インストール エンベロープ（円）はファイル Exchange からのダウンロードすることができます: https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=IOS-XR（登録ユーザのみ）。 インストール方法は、付属する .txt ファイルに記載されています。

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、IPv6 プロトコルを強化する際に、最初に Cisco 社内で対処されたものです。 その後、再び発見され、IBM Internet Security Systems X-Force の Tom Cross 氏によって報告されています。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-IPv6-leak

改訂履歴

リビジョン 1.1	2007 年 8 月 9 日	CRS-1 で稼働している IOS XR v3.4.2 についての修正情報を追加。
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

ユーザを対象としています。