Cisco Security Advisory: Cisco IOS Software IPv6 Denial of Service Vulnerability

Advisory ID: cisco-sa-20110928-ipv6

http://www.cisco.com/warp/public/707/cisco-sa-20110928-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 1.1

Last Updated 2011 September 30 2330 UTC (GMT)

For Public Release 2011 September 28 1600 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアには、 IP バージョン 6 (IPv6) プロトコル スタックの実装に関わる脆弱性が含まれます。これにより、認証されていない攻撃者は IPv6 が有効の該当デバイスをリモートから再起動できる場合があります。この脆弱性は、デバイスで不正な IPv6 パケットが処理されるときに発生する可能性があります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。この脆弱性を軽減する回避策はありません。

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-

20110928-ipv6.shtml

注：2011 年 9 月 28 日の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には 10 件の Cisco Security Advisory が含まれています。9 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決する Cisco IOS ソフトウェア リリース、および 2011 年 9 月にバンドル公開したすべての脆弱性を解決する Cisco IOS ソフトウェア リリースを記載しています。

個々の公開リンクは次のリンクにある「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」内に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep11.html

該当製品

この脆弱性の影響を受けるのは、Cisco IOS ソフトウェアが稼動し、IPv6 での運用が設定されたデバイスです。IPv6 は Cisco IOS ソフトウェアにおいてデフォルトでは有効になっていません。

脆弱性が存在する製品

該当バージョンの Cisco IOS ソフトウェアが稼動し、かつ IPv6 での運用が設定されているシスコのデバイスが影響を受けます。Cisco IOS ソフトウェアが稼動し、かつ IPv6 での運用が設定されているデバイスでは、**show ipv6 interface brief** コマンドを実行することで、IPv6 アドレスが割り当てられたいくつかのインターフェイスを表示できます。

稼動中の Cisco IOS ソフトウェアが IPv6 をサポートしていない場合、**show ipv6 interface brief** コマンドによってエラー メッセージが表示されます。または、IPv6 が有効にされていない場合は、IPv6 のインターフェイスは表示されません。このような場合、システムは脆弱性の影響を受けません。

IPv6 の運用が設定されたシステムで **show ipv6 interface brief** コマンドを実行すると、次のように出力されます。

```
router>show ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::222:90FF:FEB0:1098
    2001:DB8:2:93::3
    200A:1::1
FastEthernet0/1            [up/up]
    FE80::222:90FF:FEB0:1099
    2001:DB8:2:94::1
Serial0/0/0                [down/down]
    unassigned
Serial0/0/0.4              [down/down]
    unassigned
Serial0/0/0.5              [down/down]
    unassigned
Serial0/0/0.6              [down/down]
    unassigned
```

または、設定内に **ipv6 address <IPv6 address>** または **ipv6 enable** のインターフェイス コンフィギュレーション コマンドがある場合、IPv6 プロトコルは有効です。次の例に示すとおり、脆弱性のある設定では両方が表示されることがあります。

```
interface FastEthernet0/1
 ipv6 address 2001:0DB8:C18:1::/64 eui-64
!
interface FastEthernet0/2
 ipv6 enable
```

Cisco IOS ソフトウェアが稼動し、かつ物理または論理インターフェイス上で IPv6 での運用が設定されているデバイスの場合、**ipv6 unicast-routing** がグローバルで無効に設定されていても (つまり、デバイスが IPv6 パケットをルーティングしていない場合でも) 脆弱性の影響を受けます。

シスコ製品で稼動している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインし **show version** コマンドを実行してシステム バナーを表示させます。「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 ソフトウェアが稼動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、続いてバージョンと Cisco IOS ソフトウェア 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** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.0(1)M1 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

!--- output truncated
```

Cisco IOS ソフトウェアのリリース命名規則の追加情報は、以下のリンクの「*Cisco IOS and NX-OS Software Reference Guide*」で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性が存在しない製品

Cisco IOS XR ソフトウェアおよび Cisco IOS XE ソフトウェアは、この脆弱性の影響を受けません。

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

IPv6 は Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) が既存の IP バージョン 4 (IPv4) を置き換える目的で開発した技術です。

Cisco IOS ソフトウェアが IPv6 パケットを処理する際、脆弱性の影響を受けます。攻撃者は、IPv6 トラフィックを処理するよう設定された物理または論理インターフェイスに不正な IPv6 パケットを送信することで、この脆弱性を悪用できる可能性があります。機器を通過するトラフィックは、この脆弱性のトリガーとはなりません。この脆弱性の悪用によって、該当するシステムは再起動する可能性があります。

この脆弱性は Cisco Bug ID CSCtj41194（登録ユーザのみ）に文書化されており、Common Vulnerabilities and Exposures（CVE）ID として CVE-2011-0944 が割り当てられています。

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。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

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。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。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。

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 計算ツールを次の URL にて提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

CSCtj41194 -- Crafted IPv6 packet causes device reload Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

このアドバイザリに記載された脆弱性の不正利用に成功した場合、該当するデバイスでは再起動が発生することがあります。繰り返し不正利用されると、サービス拒否（DoS）状態が続く可能性があります。

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。

また、次のリンク先にある Cisco Security Intelligence Operations（SIO）ポータルで、Cisco IOS ソフトウェア チェッカーを入手できます。
http://tools.cisco.com/security/center/selectIOSVersion.x このツールでは、特定の Cisco IOS ソフトウェア バージョンに影響のあるセキュリティ アドバイザリを調べるための機能をいくつか提供しています。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。あるトレインが脆弱である場合、修正を含む最初のリリースは「First Fixed Release For This Advisory」列に示されます。「First Fixed Release for All Advisories in the September 2011 Bundle Publication」列は、その Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開で公開済みであるすべての脆弱性を修正する最初のリリースを示します。シスコは利用可能な最新のリリースへのアップグレードを推奨します。

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2011 Bundled Publication
There are no affected 12.0 based releases		

Affected 12.1-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2011 Bundled Publication
12.1E	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
Affected 12.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**
12.2	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2B	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2BC	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2BW	Not vulnerable	Not vulnerable
12.2BX	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2BY	Not vulnerable	Not vulnerable
12.2BZ	Not vulnerable	Not vulnerable
12.2CX	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2CY	Not vulnerable	Not vulnerable
12.2CZ	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2DA	Not vulnerable	Not vulnerable
12.2DD	Not vulnerable	Not vulnerable
12.2DX	Not vulnerable	Not vulnerable
12.2EU	Not vulnerable	Not vulnerable
12.2EW	Not vulnerable	Releases up to and including 12.2(20)EW4 are not vulnerable.
12.2E	Not vulnerable	Vulnerable; contact your

WA		support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2EX	Not vulnerable	12.2(55)EX3
12.2EY	Not vulnerable	12.2(58)EY
12.2EZ	Not vulnerable	Vulnerable; migrate to any release in 15.0SE
12.2FX	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2FY	Not vulnerable	Vulnerable; First fixed in Release 12.2EX
12.2FZ	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2IRA	Not vulnerable	Vulnerable; migrate to any release in 12.2IRG
12.2IRB	Not vulnerable	Vulnerable; migrate to any release in 12.2IRG
12.2IRC	Not vulnerable	Vulnerable; migrate to any release in 12.2IRG
12.2IRD	Not vulnerable	Vulnerable; contact your support organization per the instructions in theObtaining Fixed Software section of this advisory.
12.2IRE	Not vulnerable	Vulnerable; contact your support organization per the instructions in theObtaining Fixed Software section of this advisory.
12.2IRF	Not vulnerable	Vulnerable; migrate to any release in 12.2IRG
12.2IRG	Not vulnerable	Not vulnerable
12.2IXA	Not vulnerable	Vulnerable; contact your support organization per the instructions in theObtaining Fixed Software section of this advisory.
12.2IXB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXC	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining

		Fixed Software section of this advisory.
12.2IXD	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXE	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXF	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXG	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXH	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2JA	Not vulnerable	Not vulnerable
12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Not vulnerable
12.2MC	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2MRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRD
12.2MRB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2S	Not vulnerable	Releases prior to 12.2(30)S are vulnerable; Releases 12.2(30)S and later are not vulnerable. First fixed in Release 12.2SB
12.2SB	Not vulnerable	12.2(31)SB20 12.2(33)SB10

12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2SCA	Not vulnerable	Vulnerable; First fixed in Release 12.2SCC
12.2SCB	Not vulnerable	Vulnerable; First fixed in Release 12.2SCC
12.2SCC	Not vulnerable	12.2(33)SCC7
12.2SCD	Not vulnerable	12.2(33)SCD6
12.2SCE	Not vulnerable	12.2(33)SCE112.2(33)SCE2
12.2SCF	Not vulnerable	Not vulnerable
12.2SE	Not vulnerable	12.2(55)SE312.2(58)SE
12.2SEA	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEB	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEC	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SED	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEE	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEF	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEG	Not vulnerable	Releases prior to 12.2(25)SEG4 are vulnerable; Releases 12.2(25)SEG4 and later are not vulnerable. First fixed in Release 12.2EX
12.2SG	Not vulnerable	Releases prior to 12.2(53)SG4 are vulnerable; Releases 12.2(53)SG4 and later are not vulnerable.
12.2SGA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SL	Not vulnerable	Not vulnerable
12.2SM	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining

		Fixed Software section of this advisory.
12.2SO	Not vulnerable	Not vulnerable
12.2SQ	Not vulnerable	12.2(50)SQ3
12.2SRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRD
12.2SRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRD
12.2SRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRD
12.2SRD	Not vulnerable	12.2(33)SRD6
12.2SRE	Not vulnerable	12.2(33)SRE4
12.2STE	Not vulnerable	Not vulnerable
12.2SU	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2SV	Not vulnerable	Releases prior to 12.2(29a)SV are vulnerable; Releases 12.2(29a)SV and later are not vulnerable. Migrate to any release in 12.2SVD
12.2SVA	Not vulnerable	Not vulnerable
12.2SVC	Not vulnerable	Not vulnerable
12.2SVD	Not vulnerable	Not vulnerable
12.2SVE	Not vulnerable	Not vulnerable
12.2SW	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2SX	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2SXA	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2SXB	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2SXD	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2S	Not vulnerable	Vulnerable; First fixed in

XE		Release 12.2SXF
12.2SXF	Not vulnerable	12.2(18)SXF17b
12.2SXH	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2SXI	Not vulnerable	12.2(33)SXI6
12.2SXJ	Not vulnerable	12.2(33)SXJ1
12.2SY	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2SZ	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2T	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2TPC	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2XA	Not vulnerable	Not vulnerable
12.2XB	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2XC	Not vulnerable	Not vulnerable
12.2XD	Not vulnerable	Not vulnerable
12.2XE	Not vulnerable	Not vulnerable
12.2XF	Not vulnerable	Not vulnerable
12.2XG	Not vulnerable	Not vulnerable
12.2XH	Not vulnerable	Not vulnerable
12.2XI	Not vulnerable	Not vulnerable
12.2XJ	Not vulnerable	Not vulnerable
12.2XK	Not vulnerable	Not vulnerable

12.2XL	Not vulnerable	Not vulnerable
12.2XM	Not vulnerable	Not vulnerable
12.2XN	Not vulnerable	Not vulnerable
12.2XNA	See Cisco IOS-XE Software Availability	See Cisco IOS-XE Software Availability
12.2XNB	See Cisco IOS-XE Software Availability	See Cisco IOS-XE Software Availability
12.2XNC	See Cisco IOS-XE Software Availability	See Cisco IOS-XE Software Availability
12.2XND	See Cisco IOS-XE Software Availability	See Cisco IOS-XE Software Availability
12.2XNE	See Cisco IOS-XE Software Availability	See Cisco IOS-XE Software Availability
12.2XNF	See Cisco IOS-XE Software Availability	See Cisco IOS-XE Software Availability
12.2XO	Not vulnerable	Releases prior to 12.2(54)XO are vulnerable; Releases 12.2(54)XO and later are not vulnerable.
12.2XQ	Not vulnerable	Not vulnerable
12.2XR	Not vulnerable	Not vulnerable
12.2XS	Not vulnerable	Not vulnerable
12.2XT	Not vulnerable	Not vulnerable
12.2XU	Not vulnerable	Not vulnerable
12.2XV	Not vulnerable	Not vulnerable
12.2XW	Not vulnerable	Not vulnerable
12.2YA	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2YB	Not vulnerable	Not vulnerable
12.2YC	Not vulnerable	Not vulnerable

12.2YD	Not vulnerable	Not vulnerable
12.2YE	Not vulnerable	Not vulnerable
12.2YF	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YG	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YH	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YJ	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YK	Not vulnerable	Not vulnerable
12.2YL	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YM	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2YN	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YO	Not vulnerable	Not vulnerable
12.2YP	Not vulnerable	Not vulnerable
12.2YQ	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YR	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining

		Fixed Software section of this advisory.
12.2YS	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YT	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YU	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YV	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YW	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YX	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YY	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YZ	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZA	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2ZB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2Z	Not vulnerable	Not vulnerable

C		
12.2ZD	Not vulnerable	Not vulnerable
12.2ZE	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2ZF	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2ZG	Not vulnerable	Not vulnerable
12.2ZH	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2ZJ	Not vulnerable	Not vulnerable
12.2ZL	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZP	Not vulnerable	Not vulnerable
12.2ZU	Not vulnerable	Vulnerable; First fixed in Release 12.2SXH
12.2ZX	Not vulnerable	Not vulnerable
12.2ZY	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZYA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**

12.4	Not vulnerable	12.4(25f)
12.4 GC	12.4(24)GC4	12.4(24)GC4
12.4J A	Not vulnerable	Not vulnerable
12.4J AX	Not vulnerable	Not vulnerable
12.4J DA	Not vulnerable	Not vulnerable
12.4J DC	Not vulnerable	Not vulnerable
12.4J HA	Not vulnerable	Not vulnerable
12.4J HB	Not vulnerable	Not vulnerable
12.4J HC	Not vulnerable	Not vulnerable
12.4J K	Not vulnerable	Not vulnerable
12.4J L	Not vulnerable	Not vulnerable
12.4J MA	Not vulnerable	Not vulnerable
12.4J MB	Not vulnerable	Not vulnerable
12.4J X	Not vulnerable	Vulnerable; migrate to any release in 12.4JA Releases up to and including 12.4(21a)JX are not vulnerable.
12.4J Y	Not vulnerable	Not vulnerable
12.4 MD	Not vulnerable	12.4(24)MD6 on 28-Oct-2011
12.4 MDA	Not vulnerable	12.4(24)MDA7
12.4 MDB	Not vulnerable	12.4(24)MDB3
12.4 MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4 MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.

12.4 MRB	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4SW	Not vulnerable	Not vulnerable
12.4T	Only 12.4(24)T through 12.4(24)T4 are affected; first fixed in 12.4(24)T3c and 12.4(24)T5	12.4(24)T6 12.4(15)T16
12.4XA	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XB	Not vulnerable	12.4(2)XB12
12.4XC	Not vulnerable	Not vulnerable
12.4XD	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XE	Not vulnerable	Not vulnerable
12.4XF	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XG	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XJ	Not vulnerable	Not vulnerable
12.4XK	Not vulnerable	Not vulnerable
12.4XL	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XM	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XN	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XP	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XQ	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XR	Not vulnerable	Vulnerable; First fixed in Release 12.4T

12.4XT	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XV	Not vulnerable	Not vulnerable
12.4XW	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XY	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XZ	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4YA	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4YB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4YD	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4YE	Not vulnerable	Vulnerable; fixed in 12.4(22)YE6 on 30-Sept-2011; 12.4(24)YE7 available on 17-Oct-2011
12.4YG	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**
15.0M	15.0(1)M5	15.0(1)M7
15.0MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.0MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.

15.0S	Not vulnerable Cisco IOS XE devices: see Cisco IOS-XE Software Availability	15.0(1)S4 Cisco IOS XE devices: see Cisco IOS-XE Software Availability
15.0SA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.0SE	Not vulnerable	Not vulnerable
15.0SG	Cisco IOS XE devices: see Cisco IOS-XE Software Availability	Cisco IOS XE devices: see Cisco IOS-XE Software Availability
15.0XA	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
15.0XO	Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**
15.1EY	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.1GC	Not vulnerable	Vulnerable; First fixed in Release 15.1T
15.1M	Not vulnerable	15.1(4)M2; Available on 30-SEP-11
15.1MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.1S	Not vulnerable Cisco IOS XE devices: See Cisco IOS-XE Software Availability	15.1(2)S2 15.1(3)S Cisco IOS XE devices: See Cisco IOS-XE Software Availability

15.1T	15.1(1)T3 15.1(2)T3 15.1(3)T1	15.1(1)T4 on 09-DEC-2011 15.1(2)T4 15.1(3)T2
15.1XB	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**
There are no affected 15.2 based releases		

Cisco IOS XE ソフトウェア

Cisco IOS XE Release	First Fixed Release	First Fixed Release for All Advisories in the September 2011 Bundled Publication
2.1.x	Not vulnerable	Vulnerable; migrate to 3.3.2S or later
2.2.x	Not vulnerable	Vulnerable; migrate to 3.3.2S or later
2.3.x	Not vulnerable	Vulnerable; migrate to 3.3.2S or later
2.4.x	Not vulnerable	Vulnerable; migrate to 3.3.2S or later
2.5.x	Not vulnerable	Vulnerable; migrate to 3.3.2S or later
2.6.x	Not vulnerable	Vulnerable; migrate to 3.3.2S or later
3.1.xS	Not vulnerable	Vulnerable; migrate to 3.3.2S or later
3.1.xSG	Not vulnerable	Vulnerable; migrate to 3.2.0SG or later
3.2.xS	Not vulnerable	Vulnerable; migrate to 3.3.2S or later
3.2.xSG	Not vulnera	Not vulnerable

	ble	
3.3.xS	Not vulnerable	3.3.2S
3.4.xS	Not vulnerable	Not vulnerable

Cisco IOS XE と Cisco IOS リリースのマッピングについては、『Cisco IOS XE 2 Release Notes』、『Cisco IOS XE 3S Release Notes』、『Cisco IOS XE 3SG Release Notes』を参照してください。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2011 年 9 月のバンドル公開で説明されているいずれの脆弱性の影響も受けません。

回避策

IPv6 の設定が必要な場合、この脆弱性に対する回避策はありません。

修正済みソフトウェアの入手

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。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/en/US/docs/general/warranty/English/EU1KEN_.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。

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

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。

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

無償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と、このお知らせの URL をご用意ください。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/en/US/support/tsd_cisco_worldwide_contacts.html を参照してください。

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。

この脆弱性はシスコ内部でのテストによって発見されました。

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。

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-20110928-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-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- 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。

更新履歴

Revision 1.1	2011-September-30	Update IOS Software table bundled publication first fixed information.
Revision 1.0	2011-September-28	Initial public release.

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。