Cisco IOS の多重 DLSw サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20080326-dlsw
初公開日 : 2008-03-26 16:00
バージョン 1.5 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCsf28840 CSCsk73104

CVE-2008-1152
CVE-2007-0199

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 は特別に 巧妙に細工された UDP か IP プロトコルを処理するとき 91 のパケット メモリリークかリロードという結果に終るかもしれない Data-Link Switching （ DLSw; データリンクスイッチング ） 機能で多重 脆弱点が含まれています。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 回避策はこれらの脆弱性の効果を軽減して利用できます。

このアドバイザリは 326-dlsw で掲示されます。

注: 2008 年 3月 26 日パブリケーションは 5 つのセキュリティ アドバイザリが含まれています。 アドバイザリはすべて Cisco のインターネットワークオペレーティングシステム （ IOS ）に影響を与えます。 各アドバイザリはリリースをリストしアドバイザリに説明がある脆弱性を解決するアドバイザリはまたリリースをその正しいすべての 5 つのアドバイザリの脆弱性詳述します。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS バーチャル プライベート ダイヤルアップ ネットワーク （ VPDN ） サービス拒否の脆弱性
  326-pptp

- Cisco IOS の多重 DLSw サービス拒否の脆弱性
  326-dlsw

- IPv4/IPv6 Dual-stack ルータのための Cisco IOS User Datagram Protocol （ UDP ）配信問題
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-

IPv4IPv6

- OSPF、MPLS VPN およびスーパバイザ 32、スーパバイザ 720、または Route Switch Processor 720 の Cisco IOS の脆弱性 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue

- Cisco IOS Multicast 仮想 な プライベート ネットワーク (MVPN) データ漏洩 326-mvpn

該当製品

脆弱性のある製品

この Security Advisory は DLSw のために設定される影響を受けた Cisco IOSソフトウェアのバージョンを実行するすべてのシスコ製品に適用します。 DLSw 機能があるシステムに、有効になるそれが影響を受けていませんありませんが。

DLSw のために有効に なる ルータはローカル DLSw ピアを定義する設定で行が含まれています。 この設定はコマンド **show running-config** の発行によって観察することができます。 DLSw のために設定されるシステムは次と同じような行が含まれています:

```
dlsw local-peer
```

または

```
dlsw local-peer peer-id <IP address>
```

バージョン前の Cisco IOS のどのバージョンでもソフトウェア バージョン および 修正 下記の例にリストされている脆弱です。

デバイスに Cisco製品、ログインで動作する Cisco IOSソフトウェアのバージョンを判別し、システムバナーを表示する **show version コマンドを**発行するため。 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。 出力次の行で、イメージ名は「バージョンに」先行しているかっこと IOSリリース名の間で表示する。 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 C3640-IS-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.3(6)を実行する Cisco製品を指定したものです:

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-IS-M), Version 12.3(6), RELEASE SOFTWARE (fc3)
```

次 の 例は C3845-ADVIPSERVICESK9-M のイメージ名と Cisco IOS ソフトウェア リリース 12.3(11)T3 を実行する製品を示します:

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.3(11)T3, RELEASE
SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Cisco IOS リリース指名についてのその他の情報は http://www.cisco.com/warp/public/620/1.html で見つけることができます。

脆弱性を含んでいないことが確認された製品

DLSw のために設定されない Cisco IOSデバイスは脆弱ではないです。

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

Data-Link Switching （ DLSw; データリンク スイッチング ）は IPネットワーク上の IBM システム ネットワーク アーキテクチャ （ SNA ）および Network Basic Input/Output System （ NetBIOS (NetBIOS over IP ） ）トラフィックの転送の方法を提供します。 DLSw の Ciscoインプリメンテーションはまた高速順次転送 (FST ）のために UDP ポート 2067 および IP プロトコル 91 を使用します。

UDP および IP プロトコルを処理する 91 のパケット場合の Cisco IOS で存在 する 多重 脆弱点。これらの脆弱性は TCPパケット処理に影響を与えません。 不正利用の成功はサービス拒否 （ DoS ）に状態を導くシステムのリロードかデバイスのメモリリークという結果に終るかもしれません。

dlsw local-peer で DLSw のために設定される Cisco IOSデバイスは自動的に IP プロトコルを 91 のパケット聞き取ります。 **dlsw local-peer peer-id <IP-address>** コマンドで DLSw のために設定される Cisco IOSデバイスは IP プロトコルを 91 のパケットおよび UDP ポート 2067 聞き取ります。

Cisco IOSデバイスは IP プロトコルを DLSw が設定されるとき 91 のパケット受信します。 ただし、それは DLSw が高速順次転送 (FST ）のために設定される場合その時だけ使用されます。 DLSw FST ピア設定は次の行が含まれています:

```
dlsw remote-peer 0 fst <ip-address>
```

dlsw udp-disable コマンドで DLSw で処理する UDP をディセーブルにすることは可能性のあるです。 ただし、UDP をディセーブルにすることは UDP パケットの送信だけを防ぎます、デバイスが受信することおよび着信 UDP パケットを処理することを防ぎません。

これらの脆弱性 Cisco バグ ID CSCsk73104 （登録ユーザのみ）で文書化されています、よくある脆弱性および公開（CVE） ID CVE-2008-1152 は割り当てられました。

回避策

回避策はポート 2067 および IP プロトコルに UDP パケットのフィルタリングで 91 のパケット構成されています。 フィルタはポート 2067 にすべての IP プロトコルを 91 のパケットおよび UDP パケット フィルタリングするためにネットワーク境界で適用しますまたはユーザーによって影響を受けるデバイスで割り当てに信頼されたピア IP アドレスからだけそのようなトラフィック適用することができます。 ただし、プロトコルの両方がコネクションレス型であるので、攻撃者が正当 な ピア IP アドレスからの不正 なパケットをスプーフィングすることは可能性のあるです。

DLSw が設定されるとすぐ、Cisco IOSデバイスは IP プロトコル 91 で受信し始めます。 ただし、このプロトコルは DLSw が高速順次転送（FST）のために設定される場合その時だけ使用されます。 DLSw FST ピア設定は次の行が含まれています:

```
dlsw remote-peer 0 fst <ip-address>
```

FST が使用される場合、IP プロトコル 91 をフィルタリングすることは正当 な ピア IP アドレスからのオペレーション、従ってフィルター必要割り当てプロトコル 91 トラフィックを壊します。

dlsw udp-disable コマンドで DLSw で処理する UDP をディセーブルにすることは可能性のあるです。 ただし、UDP をディセーブルにすることは UDP パケットの送信だけを防ぎます、着信 UDP パケットの受け取り、処理を防ぎません。 脆弱 な デバイスを UDP ポート 2067 によって悪質なパケットから保護するために、次の処置の両方はとる必要があります:

1. 「dlsw udp-disable」コマンドのディセーブル UDP アウトゴーイングパケット、および
2. インフラストラクチャ ACL を使用して脆弱 な デバイスのフィルタ UDP 2067。

ネットワーク内の on Cisco 配置されたデバイスの場合もある追加緩和技術はこのアドバイザリに Cisco によって加えられる軽減情報ドキュメントガイドで利用できます:

326-dlsw

影響を受けたデバイスのコントロール プレーン ポリシングの使用

コントロール プレーン ポリシング（CoPP）がデバイスに信頼できない DLSw トラフィックをブロックするのに使用することができます。 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。 信頼できるホストを表すのに 192.168.100.1 を使用する次の例はネットワークに適応させることができます。 FST が使用されない場合、プロトコル 91 は完全にフィルタリングされるかもしれません。 UDP が **dlsw udp-disable コマンド**でディセーブルにされればさらに、UDP ポート 2067 はまた完全にフィルタリングされるかもしれません。

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses !--- configured on all interfaces
of the affected device so that !--- it will be allowed by the CoPP feature access-list 111 deny
udp host 192.168.100.1 any eq 2067 access-list 111 deny 91 host 192.168.100.1 any !--- Permit
all other DLSw traffic sent to all IP addresses !--- configured on all interfaces of the
affected device so that it !--- will be policed and dropped by the CoPP feature access-list 111
permit udp any any eq 2067 access-list 111 permit 91 any any !--- Permit (Police or Drop)/Deny
(Allow) all other Layer 3 and Layer 4 !--- traffic in accordance with existing security policies
and !--- configurations for traffic that is authorized to be sent !--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by !--- the CoPP feature class-map match-all
drop-DLSw-class match access-group 111 !--- Create a Policy-Map that will be applied to the !---
Control-Plane of the device. policy-map drop-DLSw-traffic class drop-DLSw-class drop !--- Apply
the Policy-Map to the Control-Plane of the !--- device control-plane service-policy input drop-
DLSw-traffic
```

CoPP 上の例では、「拒否」操作を一致するパケットは policy-map ドロップする 機能から（示されていない）影響を受けないが policy-map 「ドロップする」機能によって廃棄されるこれらのパケットの「割り当て」アクションの結果を用いる潜在的なエクスプロイト パケットを一致する アクセス制御エントリ（ACE）。 以下の事項に注意して下さい: Cisco IOS 12.2S および 12.0S で policy-map 構文を異なっていますトレインします:

```
policy-map drop-DLSw-traffic
 class drop-DLSw-class
  police 32000 1500 1500 conform-action drop exceed-action drop
```

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 で利用できます。

ネットワーク境界のインフラストラクチャ ACL の使用

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。 iACLs はネットワーク セキュリティ 最良 の 方法で、よいネットワーク セキュリティへの長期付加、またこの特定の脆弱性のための回避策として考慮する必要があります。 下記に示されている iACL 例はインフラストラクチャ IPアドレス範囲の IP アドレスのすべてのデバイスを保護する展開されたインフラストラクチャ access-list の一部として含まれるはずです。 FST が使用されない場合、プロトコル 91 は完全にフィルタリングされるかもしれません。 UDP が **dlsw udp-disable コマンド**でディセーブルにされればさらに、UDP ポート 2067 はまた完全にフィルタリングされるかもしれません。

```
!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets !--- from trusted hosts destined to
infrastructure addresses. access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES
MASK eq 2067 access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK !---
Deny DLSw (UDP port 2067 and IP protocol 91) packets from !--- all other sources destined to
infrastructure addresses. access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 deny 91 any INFRASTRUCTURE_ADDRESSES MASK !--- Permit/deny all other Layer 3 and
Layer 4 traffic in accordance !--- with existing security policies and configurations !---
Permit all other traffic to transit the device. access-list 150 permit ip any any interface
serial 2/0 ip access-group 150 in
```

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。 このホワイトペーパーは、以下のリンクから入手可能です。

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

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center (TAC) または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表 (下掲) の各行には、Cisco IOS のリリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース (および、それぞれの予想提供日) が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い (第 1 修正済みリリースより古い) トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	修正済みリリースの入手可能性	
Affected 12.0-Based Releases	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.0	脆弱性あり; first fixed in 12.3	12.3(26)
12.0DA	Release prior to 12.0(8)DA3 are vulnerable， releases 12.0(8)DA3 and later are not vulnerable; migrate to any release in 12.2DA	

12.0DB	Release prior to 12.0(7)DB are vulnerable， releases 12.0(7)DB and later are not vulnerable; first fixed in 12.4	12.4(18a)
12.0DC	Release prior to 12.0(7)DC are vulnerable， releases 12.0(7)DC and later are not vulnerable; first fixed in 12.4	12.4(18a)
12.0S	Release prior to 12.0(17)S5 are vulnerable， releases 12.0(17)S5 and later are not vulnerable;	
12.0SC	脆弱性なし	
12.0SL	脆弱性なし	
12.0SP	脆弱性なし	
12.0ST	脆弱性なし	
12.0SX	脆弱性なし	
12.0SY	脆弱性なし	
12.0SZ	脆弱性なし	
12.0T	脆弱性あり; first fixed in 12.3	12.3(26)
12.0W	脆弱性あり; contact TAC	12.0(3c) W5(8)
12.0WC	脆弱性あり; contact TAC	
12.0WT	脆弱性なし	
12.0XA	脆弱性あり; first fixed in 12.3	12.3(26)
12.0XB	脆弱性なし	
12.0XC	Release prior to 12.0(2)XC2 are vulnerable， releases 12.0(2)XC2 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.0XD	脆弱性あり; first fixed in 12.3	12.3(26)
12.0XE	脆弱性あり; first fixed in 12.1E	
12.0XF	脆弱性なし	
12.0XG	脆弱性あり; first fixed in 12.3	12.3(26)
12.0XH	脆弱性あり; first fixed in 12.3	12.3(26)
12.0XI	Release prior to 12.0(4)XI2 are vulnerable， releases 12.0(4)XI2 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.0XJ	Release prior to 12.0(4)XJ5 are vulnerable， releases 12.0(4)XJ5 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.0XK	脆弱性あり; first fixed in 12.3	12.3(26)
12.0XL	脆弱性なし	
12.0XM	脆弱性なし	

12.0XN	脆弱性あり; first fixed in 12.3	12.3(26)
12.0XQ	脆弱性あり; first fixed in 12.3	12.3(26)
12.0XR	脆弱性あり; first fixed in 12.3	12.3(26)
12.0XS	脆弱性なし	
12.0XV	脆弱性なし	
12.0XW	脆弱性なし	
Affected 12.1-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.1	脆弱性あり; first fixed in 12.3	12.3(26)
12.1AA	脆弱性あり; first fixed in 12.3	12.3(26)
12.1AX	脆弱性なし	
12.1AY	Release prior to 12.1(22)AY1 are vulnerable， releases 12.1(22)AY1 and later are not vulnerable;	12.1(22)EA11
12.1AZ	脆弱性なし	
12.1CX	脆弱性なし	
12.1DA	脆弱性なし	
12.1DB	Release prior to 12.1(4)DB1 are vulnerable， releases 12.1(4)DB1 and later are not vulnerable; first fixed in 12.4	12.4(18a)
12.1DC	Release prior to 12.1(4)DC2 are vulnerable， releases 12.1(4)DC2 and later are not vulnerable; first fixed in 12.4	12.4(18a)
12.1E	12.1(27b)E4	
12.1EA	Release prior to 12.1(11)EA1 are vulnerable， releases 12.1(11)EA1 and later are not vulnerable;	12.1(22)EA11
12.1EB	脆弱性なし	
12.1EC	脆弱性あり; migrate to any release in 12.2BC	12.3(23)BC1
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	脆弱性あり; first fixed in 12.1E	
12.1EY	脆弱性なし	
12.1EZ	脆弱性あり; first fixed in 12.1E	
12.1GA	脆弱性あり; first fixed in 12.3	12.3(26)
12.1GB	脆弱性あり; first fixed in 12.3	12.3(26)
12.1T	脆弱性あり; first fixed in 12.3	12.3(26)

12.1XA	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XB	脆弱性なし	
12.1XC	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XD	脆弱性あり; first fixed in 12.3	12.3(26)
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	12.3(26)
12.1XH	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XI	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XJ	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XK	脆弱性なし	
12.1XL	脆弱性なし	
12.1XM	脆弱性あり; first fixed in 12.3	12.3(26)
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	12.3(26)
12.1XQ	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XR	脆弱性なし	
12.1XS	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XT	Release prior to 12.1(3)XT2 are vulnerable， releases 12.1(3)XT2 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.1XU	脆弱性なし	
12.1XV	Release prior to 12.1(5)XV1 are vulnerable， releases 12.1(5)XV1 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.1XW	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XX	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XY	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XZ	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YA	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YB	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YC	脆弱性なし	
12.1YD	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YE	Release prior to 12.1(5)YE1 are vulnerable， releases 12.1(5)YE1 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.1YF	脆弱性なし	
12.1YG	脆弱性なし	
12.1YH	脆弱性なし	
12.1YI	脆弱性あり; first fixed in 12.3	12.3(26)

12.1YJ	脆弱性なし	
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
12.2	脆弱性あり; first fixed in 12.3	12.3(26)
12.2B	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2BC	脆弱性なし	
12.2BW	脆弱性あり; first fixed in 12.3	12.3(26)
12.2BY	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2BZ	脆弱性なし	
12.2CX	脆弱性なし	
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 12.4	12.4(18a)
12.2DX	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2EU	脆弱性なし	
12.2EW	脆弱性なし	
12.2EWA	脆弱性なし	
12.2EX	Release prior to 12.2(20)EX are vulnerable， releases 12.2(20)EX and later are not vulnerable; migrate to any release in 12.2SEA	12.2(40)EX1
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	脆弱性あり; contact TAC	
12.2IXB	脆弱性あり; contact TAC	
12.2IXC	脆弱性あり; contact TAC	
12.2IXD	脆弱性あり; contact TAC	
12.2IXE	脆弱性あり; migrate to any release in 12.2IXF	12.2(18)IXF; 31-MAR-08 で利用可能
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)MC2k
12.2S	12.2(25)S15	12.2(25)S15
12.2SB	12.2(28)SB10 12.2(31)SB9 12.2(33)SB; 31-MAR-2008 で利用可能	12.2(31)SB11
12.2SBC	脆弱性あり; first fixed in 12.2SB; 31-MAR-2008 で利用可能	12.2(31)SB11
12.2SCA	脆弱性なし	
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(44)SG	12.2(44)SG
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	12.2(33)SRA6	12.2(33)SRA7
12.2SRB	12.2(33)SRB3; 07-APR-2008 で利用可能	12.2(33)SRB3; 14-APR-08 で利用可能
12.2SRC	脆弱性なし	
12.2SU	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2SV	Release prior to 12.2(29a)SV1 are vulnerable， releases 12.2(29a)SV1 and later are not vulnerable; migrate	12.2(29b)SV

	to any release in 12.2SVA	
12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	
12.2SVD	脆弱性なし	
12.2SW	Release prior to 12.2(25)SW10 are vulnerable， releases 12.2(25)SW10 and later are not vulnerable;	
12.2SX	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXB	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXD	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXE	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXF	12.2(18)SXF12 12.2(18)SXF12a	12.2(18)SXF13
12.2SXH	12.2(33)SXH1	12.2(33)SXH2
12.2SY	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SZ	脆弱性あり; first fixed in 12.2S	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2T	脆弱性あり; first fixed in 12.3	12.3(26)
12.2TPC	12.2(8)TPC10d	
12.2UZ	脆弱性なし	
12.2XA	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XB	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XC	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2XD	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XE	脆弱性なし	
12.2XF	脆弱性なし	
12.2XG	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XH	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XI	脆弱性なし	
12.2XJ	脆弱性あり; first fixed in 12.3	12.3(26)

12.2XK	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XL	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XM	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XN	12.2(33)XN1	12.3(26)
12.2XO	脆弱性なし	
12.2XQ	脆弱性あり; first fixed in 12.3	12.3(26)
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	12.3(26)
12.2XU	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XV	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XW	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YA	Release prior to 12.2(4)YA8 are vulnerable， releases 12.2(4)YA8 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.2YB	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YC	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YD	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YE	脆弱性あり; first fixed in 12.2S	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2YF	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YG	脆弱性なし	
12.2YH	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YJ	Release prior to 12.2(8)YJ1 are vulnerable， releases 12.2(8)YJ1 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.2YK	脆弱性なし	
12.2YL	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YM	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YN	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YO	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2YP	脆弱性なし	
12.2YQ	脆弱性なし	
12.2YR	脆弱性なし	
12.2YS	脆弱性なし	
12.2YT	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YU	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YV	Release prior to 12.2(11)YV1 are	12.4(18a)

	vulnerable， releases 12.2(11)YV1 and later are not vulnerable; first fixed in 12.4	
12.2YW	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YX	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YY	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YZ	脆弱性あり; first fixed in 12.2S	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2ZA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2ZB	脆弱性あり; first fixed in 12.4	12.4(18a)
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	12.3(26)
12.2ZF	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2ZG	脆弱性なし	
12.2ZH	Release prior to 12.2(13)ZH6 are vulnerable， releases 12.2(13)ZH6 and later are not vulnerable; first fixed in 12.4	12.2(13)ZH11
12.2ZJ	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2ZL	脆弱性あり; first fixed in 12.4	12.4(15)T4 12.4(18a)
12.2ZP	脆弱性なし	
12.2ZU	脆弱性あり; first fixed in 12.2SXH	12.2(33)SXH2
12.2ZY	12.2(18)ZY2	12.2(18)ZY2
Affected 12.3-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.3	12.3(24)	12.3(26)
12.3B	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3BC	脆弱性なし	
12.3BW	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3EU	脆弱性なし	
12.3JA	脆弱性なし	
12.3JEA	脆弱性なし	

12.3JEB	脆弱性なし	
12.3JEC	脆弱性なし	
12.3JK	Release prior to 12.3(8)JK1 are vulnerable， releases 12.3(8)JK1 and later are not vulnerable;	12.3(8)JK1
12.3JL	脆弱性なし	
12.3JX	脆弱性なし	
12.3T	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3TPC	脆弱性なし	
12.3VA	脆弱性あり; contact TAC	
12.3XA	12.3(2)XA7; 31-MAR-2008 で利用可能	12.3(2)XA7; 31-MAR-08 で利用可能
12.3XB	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XC	12.3(2)XC5	12.4(15)T4 12.4(18a)
12.3XD	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XE	12.3(2)XE6; 31-MAR-2008 で利用可能	12.4(15)T4 12.4(18a)
12.3XF	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XG	脆弱性あり; first fixed in 12.3YG; 16-JUN-2008 で利用可能	12.4(15)T4 12.4(18a)
12.3XH	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XI	12.3(7)XI11; 18-SEP-2008 で利用可能	
12.3XJ	脆弱性あり; first fixed in 12.3YX	12.3(14)YX11 12.4(15)T4
12.3XK	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XQ	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XR	12.3(7)XR8; 31-MAR-2008 で利用可能	12.3(7)XR8; 31-MAR-08 で利用可能
12.3XS	脆弱性なし	
12.3XU	脆弱性あり; first fixed in 12.4T	12.4(15)T4

12.3XW	脆弱性あり; first fixed in 12.3YX	12.3(14)YX11 12.4(15)T4
12.3XY	脆弱性なし	
12.3YA	脆弱性なし	
12.3YD	脆弱性なし	
12.3YF	脆弱性あり; first fixed in 12.3YX	12.3(14)YX11 12.4(15)T4
12.3YG	12.3(8)YG7; 16-JUN-2008 で利用可能	12.4(15)T4
12.3YH	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YI	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YJ	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YK	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YM	12.3(14)YM12	12.3(14)YM12
12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YS	12.3(11)YS3; 31-MAR-2008 で利用可能	12.4(15)T4
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YU	脆弱性あり; first fixed in 12.4XB	
12.3YX	12.3(14)YX11	12.3(14)YX11
12.3YZ	12.3(11)YZ3	
Affected 12.4-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.4	12.4(10c) 12.4(13e) 12.4(16b) 12.4(17) 12.4(3h) 12.4(8d)	12.4(18a)
12.4JA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JMA	脆弱性なし	

12.4JMB	脆弱性なし	
12.4JMC	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	脆弱性なし	
12.4SW	脆弱性あり; contact TAC	12.4(15)SW
12.4T	12.4(15)T2 12.4(6)T10 12.4(9)T7	12.4(15)T4
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.4XB	12.4(2)XB6	
12.4XC	脆弱性あり; contact TAC	
12.4XD	12.4(4)XD10	12.4(4)XD10
12.4XE	12.4(6)XE2	12.4(15)T4
12.4XF	脆弱性なし	
12.4XG	12.4(9)XG2	12.4(9)XG2
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.4XK	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.4XL	12.4(15)XL2	12.4(15)XL2
12.4XM	脆弱性なし	
12.4XN	脆弱性なし	
12.4XT	12.4(6)XT2	12.4(6)XT2
12.4XV	12.4(11)XV	
12.4XW	脆弱性あり; contact TAC	12.4(11)XW6
12.4XY	脆弱性なし	

Cisco IOSソフトウェア モジュール性のための特別なパッチは 12.2(18)SXF11 にまた利用でき、http://tools.cisco.com/swdf/ionpn/jsp/result.jsp?s_tarballWild=mp001-p.122-18.SXF11&reqType=cWork の Cisco IOSソフトウェア モジュール性パッチ ナビゲーターからダウンロードすることができます。

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。

これらの脆弱性は内部で発見されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-dlsw

改訂履歴

Revision 1.5	2008-June-26	リンクおよび冗漫を取除く更新済要約。
リビジョン 1.4	2008-April-25	CSCsk73104 の CVSS スコアへの更新済リンク。
リビジョン 1.3	2008-Apr-21	IOS software モジュール性パッチへの特定のリンクを追加しました
リビジョン 1.2	2008-Mar-31	正しい表と IOS 第 1 固定表を取り替えること -- 不正確な 3/28 と 3/31was 間で目に見えるデータ
リビジョン 1.1	2008-Mar-29	advisory ID cisco-sa-20080326-IPv4IPv6 の新しい情報による 12.0S、12.0SY、12.0SX および 12.0SZ のための更新済ソフトウェア テーブル IPv4IPv6 デュアルスタック ルータの行進第 26 アドバイザリ。
リビジョン 1.0	2008-Mar-26	初版リリース

利用規約