

Cisco IOS MPLS VPN は情報をリークさせるかもしれません

Medium	アドバイザリーID : cisco-sa-20080924-vpn	CVE-2008-3803
m	初公開日 : 2008-09-24 16:00	
	バージョン 1.2 : Final	
	CVSSスコア : 5.1	
	回避策 : Yes	
	Cisco バグ ID : CSCec12299 , CSCee83237	

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バージョン 12.0S を、12.2、12.3 か 12.4 およびマルチプロトコル ラベル スイッチング (MPLS) バーチャルプライベート ネットワーク (VPN) か VPN Routing and Forwarding ライト (VRF ライト) のために設定されて実行し、Customer Edge (CE) および Provider Edge (PE) デバイス間のボーダー ゲートウェイ プロトコル (BGP) を使用するデバイスは情報が VPN の間で伝搬するようにするかもしれません。

回避策はこの脆弱性の軽減を助けて利用できます。

この問題は論理エラーによって PE デバイスの extended community を処理するとき引き起こされます。

この問題は攻撃者によって決定論的に不正利用することができません。

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。これらの脆弱性に対しては回避策があります。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn> で掲示されます。

2008 年 9 月 24 日 IOS アドバイザリーによって組み込まれる書は 12 のセキュリティ アドバイザリーが含まれています。アドバイザリーの 11 は Cisco の IOS software の脆弱性に対処し、1 つのアドバイザリーは Cisco Unified Communications Manager の脆弱性に対処します。各アドバイザリーはリリースをリストしますアドバイザリーに説明がある脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosips>
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl>
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip>
- [924-cucm](#)
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi>
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc>
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr>
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast>
- [924-sccp](#)
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosfw>
- [924-l2tp](#)

該当製品

修正済みソフトウェア

Cisco IOSデバイスは MPLS VPN が VRF ライトのために設定され、CE および PE デバイス間の BGPセッションがあり、extended community を処理し脆弱。デバイスが MPLS VPN が VRF ライトのためにコマンド `address-family ipv4 vrf <vrf 名前>` または設定されるか、`address-family ipv6 VRF <vrf 名前は>` デバイスコンフィギュレーションにあります。

以下は MPLS VPN のために設定されるデバイスで実行されるコマンドを示します:

```
router#show running-config | include address-family [ipv4|ipv6]
address-family ipv4 vrf <vrf-name>
```

以下は PE と CE 間の IPv4 BGPセッションのために設定される PE デバイスを示します:

```
router#show running-config | include address-family [ipv4|ipv6]
address-family ipv4 vrf <vrf-name>
```

デバイスに Cisco製品、ログインで動作するソフトウェアを判別し、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」先行しているかこと IOSリリース名の間で表示する。他の Ciscoデバイスに"show version" コマンドがありませんまたはために別の出力を与えて下さい。

次の例は Cisco IOS Release 12.4(11)T2 を実行している Cisco製品を指定したものです:

```
Router#show version
Cisco IOS Software, 7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(11)T2, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
```

<output truncated>

Cisco IOSリリース命名規則のその他の情報は「白書と資格を与えられる文書で見つけることができます: <http://www.cisco.com/web/about/security/intelligence/ios-ref.html> で利用可能である Cisco IOSレファレンスガイド」、

脆弱性を含んでいないことが確認された製品

MPLS VPNs のために設定されないシスコ製品が VRF ライトはこの脆弱性によって変化しないです。

IOS を実行しないシスコ製品はこの脆弱性によって変化しないです。

Cisco IOS XR は影響を受けていません。

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。

改訂履歴

リビジョン 1.2	2009- April-16	現在旧式であるように、結合されたソフトウェア テーブルへの取除かれた参照。
リビジョン 1.1	2008- Nov-19	回避策 セクションの更新済設定例。
リビジョン 1.0	2008- Sep-24	初回公開リリース

利用規約

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も示唆するものではありません。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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。