

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Advisories](#)

# Cisco Security Advisory: Cisco IOS MPLS VPN May Leak Information

Advisory ID: cisco-sa-20080924-vpn

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>

## Revision 1.2

Last Updated 2009 April 16 2100 UTC (GMT)

For Public Release 2008 September 24 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

---

## Summary

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>.

The September 24, 2008 IOS Advisory bundled publication includes twelve Security Advisories. Eleven of the advisories address vulnerabilities in Cisco's IOS software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each Advisory lists the releases that correct the vulnerability described in the Advisory.

Individual publication links are listed below:

- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ubr.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml>

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

## ☐ Affected Products

Products running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for MPLS VPNs or VRF Lite are potentially affected.

Cisco IOS releases based on 12.1 are not affected.

## ☐ Vulnerable Products

Cisco IOS devices are vulnerable if they are configured for MPLS VPN or VRF Lite and have a BGP session between the CE and PE devices, and process extended communities. If a device is configured for MPLS VPN or VRF Lite the command **address-family ipv4 vrf <vrf-name>** or **address-family ipv6 vrf <vrf-name>** will be present in the device configuration.

The following shows a command executed on a device configured for MPLS VPN:

```
router#show running-config | include address-family [ipv4|ipv6]
```

```
address-family ipv4 vrf <vrf-name>
```

The following shows a PE device configured for an IPv4 BGP session between the PE and the CE:

```
router bgp <Local AS>
  address-family ipv4 vrf one
  neighbor <neighbor IP> remote-as < Remote AS>
  neighbor <neighbor IP> activate
```

To determine the software running on a Cisco product, log in to the device and issue the "show version" command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the "show version" command or will give different output.

The following example identifies a Cisco product that is running Cisco IOS release 12.4(11)T2:

```
Router#show version
Cisco IOS Software, 7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(1
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 01-May-07 04:19 by prod_rel_team

<output truncated>
```

Additional information on the Cisco IOS release naming conventions can be found on the document entitled "White Paper: Cisco IOS Reference Guide", which is available at <http://www.cisco.com/warp/public/620/1.html>

## ☐ Products Confirmed Not Vulnerable

Cisco products not configured for MPLS VPNs or VRF Lite are unaffected by this vulnerability.

Cisco products that do not run IOS are unaffected by this vulnerability.

Cisco IOS-XR is not affected.

No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#)   [Close Section](#)

## ☐ Details

MPLS VPNs allow for the creation of 'virtual networks' that customers can use to segregate traffic into multiple, isolated VPNs. Traffic within each MPLS VPN is kept separate from the others, thereby maintaining a virtual private network.

More information on MPLS and MPLS VPNs is available at the following link:

[http://www.cisco.com/en/US/products/ps6557/products\\_ios\\_technology\\_home.html](http://www.cisco.com/en/US/products/ps6557/products_ios_technology_home.html)

A bug exists when processing extended communities with MPLS VPNs. If extended communities are used, MPLS VPN may incorrectly use a corrupted route target (RT) to forward traffic. If this occurs, traffic can leak from one MPLS VPN to another.

This vulnerability exists whenever an affected PE device has a BGP session running in the MPLS VPN Virtual Routing and Forwarding (VRF). The following two examples of this scenario are the most common:

- 1) MPLS VPN configuration with BGP running inside the VRF between the PE and CE devices.
- 2) MPLS Inter-AS option A with BGP running between the Autonomous System Border Routers (ASBR).

The mitigation in the Workarounds section filters extended communities on a PE device, preventing them from being received by devices configured for MPLS VPN.

This vulnerability was introduced with Cisco bug ID CSCee83237. Cisco IOS images that do not include CSCee83237 are not vulnerable to this issue.

It is important to note that this condition cannot be triggered by an attacker and that the condition does not provide ways to determine the flow of traffic between VPNs.

This vulnerability is documented in the Cisco Bug ID [CSCec12299](#) ( [registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2008-3803.

[Top of the section](#)   [Close Section](#)

## ☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

<b>CSCec12299 - Corruption of ext communities when receiving over ipv4 EBGP session</b>					
Calculate the environmental score of <a href="#">CSCec12299</a>					
CVSS Base Score - <b>5.1</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	Partial	Partial	Partial
CVSS Temporal Score - <b>4.2</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#)   [Close Section](#)

## ☐ Impact

This vulnerability may cause traffic to be improperly routed between MPLS VPNs, which may lead to a breach of confidentiality.

[Top of the section](#)   [Close Section](#)

## ☐ Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based	First Fixed Release	Recommended Release

Releases		
12.0	Not Vulnerable	
12.0DA	Not Vulnerable	
12.0DB	Not Vulnerable	
12.0DC	Not Vulnerable	
12.0S	12.0(30)S5 12.0(31)S3 12.0(32)S	12.0(32)S11 12.0(33)S1
12.0SC	Not Vulnerable	
12.0SL	Not Vulnerable	
12.0SP	Not Vulnerable	
12.0ST	Not Vulnerable	
12.0SX	Vulnerable; first fixed in <a href="#">12.0S</a>	12.0(32)S11 12.0(33)S1
12.0SY	Not Vulnerable	
12.0SZ	12.0(30)SZ4	12.0(32)S11 12.0(33)S1
12.0T	Not Vulnerable	
12.0W	Not Vulnerable	
12.0WC	Not Vulnerable	
12.0WT	Not Vulnerable	
12.0XA	Not Vulnerable	
12.0XB	Not Vulnerable	
12.0XC	Not Vulnerable	
12.0XD	Not Vulnerable	
12.0XE	Not Vulnerable	
12.0XF	Not Vulnerable	
12.0XG	Not Vulnerable	
12.0XH	Not Vulnerable	
12.0XI	Not Vulnerable	
12.0XJ	Not Vulnerable	
12.0XK	Not Vulnerable	

12.0XL	Not Vulnerable	
12.0XM	Not Vulnerable	
12.0XN	Not Vulnerable	
12.0XQ	Not Vulnerable	
12.0XR	Not Vulnerable	
12.0XS	Not Vulnerable	
12.0XT	Not Vulnerable	
12.0XV	Not Vulnerable	
<b>Affected 12.1-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.1 based releases		
<b>Affected 12.2-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.2	Not Vulnerable	
12.2B	Not Vulnerable	
12.2BC	Not Vulnerable	
12.2BW	Not Vulnerable	
12.2BX	Not Vulnerable	
12.2BY	Not Vulnerable	
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Not Vulnerable	
12.2DA	Not Vulnerable	
12.2DD	Not Vulnerable	
12.2DX	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	
12.2EX	Not Vulnerable	
12.2EY	Not Vulnerable	
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	

12.2FZ	Not Vulnerable	
12.2IRB	Not Vulnerable	
12.2IXA	Vulnerable; migrate to any release in 12.2IXD	12.2(18)IXG
12.2IXB	Vulnerable; migrate to any release in 12.2IXD	12.2(18)IXG
12.2IXC	Vulnerable; migrate to any release in 12.2IXD	12.2(18)IXG
12.2IXD	Not Vulnerable	
12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2IXG	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	
12.2S	12.2(30)S and later are vulnerable. 12.2(25)S and before are not vulnerable	12.2(33)SB2; Available on 26-SEP-08
12.2SB	12.2(28)SB5 12.2(31)SB2 12.2(31)SB3x	12.2(33)SB2; Available on 26-SEP-08
12.2SBC	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB2; Available on 26-SEP-08
12.2SCA	Not Vulnerable	
12.2SE	Not Vulnerable	
12.2SEA	Not Vulnerable	
12.2SEB	Not Vulnerable	
12.2SEC	Not Vulnerable	
12.2SED	Not Vulnerable	
12.2SEE	Not Vulnerable	

12.2SEF	Not Vulnerable	
12.2SEG	Not Vulnerable	
12.2SG	12.2(37)SG	12.2(46)SG1
12.2SGA	12.2(31)SGA8	12.2(31)SGA8
12.2SL	Not Vulnerable	
12.2SM	12.2(29)SM2	12.2(29)SM4
12.2SO	Not Vulnerable	
12.2SRA	Not Vulnerable	
12.2SRB	Not Vulnerable	
12.2SRC	Not Vulnerable	
12.2SU	Not Vulnerable	
12.2SV	12.2(29b)SV1	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Not Vulnerable	
12.2SXE	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF15
12.2SXF	12.2(18)SXF3	12.2(18)SXF15
12.2SXH	Not Vulnerable	
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Not Vulnerable	
12.2TPC	Not Vulnerable	
12.2XA	Not Vulnerable	
12.2XB	Not Vulnerable	
12.2XC	Not Vulnerable	
12.2XD	Not Vulnerable	
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	

12.2XG	Not Vulnerable	
12.2XH	Not Vulnerable	
12.2XI	Not Vulnerable	
12.2XJ	Not Vulnerable	
12.2XK	Not Vulnerable	
12.2XL	Not Vulnerable	
12.2XM	Not Vulnerable	
12.2XN	Not Vulnerable	
12.2XNA	Not Vulnerable	
12.2XNB	Not Vulnerable	
12.2XO	Not Vulnerable	
12.2XQ	Not Vulnerable	
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Not Vulnerable	
12.2XU	Not Vulnerable	
12.2XV	Not Vulnerable	
12.2XW	Not Vulnerable	
12.2YA	Not Vulnerable	
12.2YB	Not Vulnerable	
12.2YC	Not Vulnerable	
12.2YD	Not Vulnerable	
12.2YE	Not Vulnerable	
12.2YF	Not Vulnerable	
12.2YG	Not Vulnerable	
12.2YH	Not Vulnerable	
12.2YJ	Not Vulnerable	
12.2YK	Not Vulnerable	
12.2YL	Not Vulnerable	
12.2YM	Not Vulnerable	
12.2YN	Not Vulnerable	
12.2YO	Not Vulnerable	
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	

12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Not Vulnerable	
12.2YU	Not Vulnerable	
12.2YV	Not Vulnerable	
12.2YW	Not Vulnerable	
12.2YX	Not Vulnerable	
12.2YY	Not Vulnerable	
12.2YZ	Not Vulnerable	
12.2ZA	Not Vulnerable	
12.2ZB	Not Vulnerable	
12.2ZC	Not Vulnerable	
12.2ZD	Not Vulnerable	
12.2ZE	Not Vulnerable	
12.2ZF	Not Vulnerable	
12.2ZG	Not Vulnerable	
12.2ZH	Not Vulnerable	
12.2ZJ	Not Vulnerable	
12.2ZL	Not Vulnerable	
12.2ZP	Not Vulnerable	
12.2ZU	Not Vulnerable	
12.2ZX	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB2; Available on 26-SEP-08
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.3	Not Vulnerable	
12.3B	Not Vulnerable	
12.3BC	Not Vulnerable	
12.3BW	Not Vulnerable	
12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	

12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	
12.3JK	Not Vulnerable	
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	
12.3T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3TPC	Not Vulnerable	
12.3VA	Not Vulnerable	
12.3XA	Not Vulnerable	
12.3XB	Not Vulnerable	
12.3XC	Not Vulnerable	
12.3XD	Not Vulnerable	
12.3XE	Not Vulnerable	
12.3XF	Not Vulnerable	
12.3XG	Not Vulnerable	
12.3XI	Not Vulnerable	
12.3XJ	Not Vulnerable	
12.3XK	Not Vulnerable	
12.3XL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XQ	Not Vulnerable	
12.3XR	Not Vulnerable	
12.3XS	Not Vulnerable	
12.3XU	Not Vulnerable	
12.3XW	Not Vulnerable	
12.3XX	Not Vulnerable	
12.3XY	Not Vulnerable	
12.3XZ	Not Vulnerable	
12.3YA	Not Vulnerable	
12.3YD	Not Vulnerable	
		12.3(14)YX13

12.3YF	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.4(15)T7
12.3YG	Not Vulnerable	
12.3YH	Not Vulnerable	
12.3YI	Not Vulnerable	
12.3YJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.3YK	12.3(11)YK3	12.4(15)T7
12.3YM	12.3(14)YM10	12.3(14)YM13; Available on 30-SEP-08
12.3YQ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.3YS	12.3(11)YS2	12.4(15)T7
12.3YT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.3YU	Vulnerable; first fixed in <a href="#">12.4XB</a>	12.4(2)XB10
		12.4(9)XG3
		12.4(15)T7
12.3YX	12.3(14)YX7	12.3(14)YX13
12.3YZ	12.3(11)YZ2	
12.3ZA	Not Vulnerable	
<b>Affected 12.4-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	12.4(10c) 12.4(12a) 12.4(13) 12.4(3h) 12.4(5c) 12.4(7e) 12.4(8d)	12.4(18c)
12.4JA	Not Vulnerable	

12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JMC	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	12.4(11)SW1	12.4(15)SW2; Available on 28- SEP-08
12.4T	12.4(11)T2 12.4(15)T 12.4(2)T6 12.4(4)T8 12.4(6)T7 12.4(9)T3	12.4(15)T7
12.4XA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XB	12.4(2)XB6	12.4(2)XB10
12.4XC	12.4(4)XC7	12.4(15)T7
12.4XD	12.4(4)XD7	12.4(4)XD11; Available on 26- SEP-08
12.4XE	12.4(6)XE3	12.4(15)T7
12.4XF	Not Vulnerable	
12.4XG	12.4(9)XG2	12.4(9)XG3
12.4XJ	12.4(11)XJ2	12.4(15)T7
12.4XK	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
	Vulnerable; contact	

12.4XP	TAC	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	12.4(6)XT1	12.4(15)T7
12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	Not Vulnerable	
12.4XZ	Not Vulnerable	
12.4YA	Not Vulnerable	

[Top of the section](#)   [Close Section](#)

## Workarounds

Customers running versions of Cisco IOS that support filtering of extended communities can prevent the corruption of the route target (RT) by applying a BGP route-map that removes RT entries on inbound BGP sessions.

The following configuration example applied in the ipv4 address family of a PE device removes extended communities from the CE router:

```
router bgp <Local AS>
  address-family ipv4 vrf one
  neighbor <neighbor IP> remote-as <Remote AS>
  neighbor <neighbor IP> activate
  neighbor <neighbor IP> route-map FILTER in
  exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
  set extcomm-list 100 delete
!
```

The following configuration example applied in the ipv6 address family of a PE device removes extended communities from the CE router:

```
router bgp <Local AS>
  address-family ipv6 vrf one
  neighbor <neighbor IP> remote-as <Remote AS>
  neighbor <neighbor IP> activate
  neighbor <neighbor IP> route-map FILTER in
  exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
```

```
set extcomm-list 100 delete
!
```

**Note:** The capability of filtering extended communities is only available in certain 12.0S and 12.2S based Cisco IOS releases.

BGP session between the PE and the CE needs to be cleared to make this configuration change effective.

[Top of the section](#)   [Close Section](#)

## ☐ **Obtaining Fixed Software**

Cisco has released free software updates that address these vulnerabilities. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at [http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto:security-alert@cisco.com) for software upgrades.

### ☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

### ☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

### ☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical

Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#)   [Close Section](#)

## ☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by a customer.

This vulnerability cannot be deterministically triggered by an attacker.

[Top of the section](#)   [Close Section](#)

## ☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#)   [Close Section](#)

## ☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#)   [Close Section](#)

## ☐ Revision History

Revision 1.2	2009-April-16	Removed references to the combined software table, as it is now outdated.
Revision 1.1	2008-Nov-19	Updated configuration examples in <a href="#">Workarounds</a> section.
Revision 1.0	2008-Sep-24	Initial public release.

[Top of the section](#)   [Close Section](#)

## ☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#)   [Close Section](#)

---

**Help us help you.**



**Please rate this document.**

- Excellent
- Good
- Average
- Fair
- Poor

**This document solved my problem.**

- Yes
- No
- Just browsing

**Suggestions for improvement:**

(256 character limit)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)