

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

Security Advisories

# Cisco Security Advisory: Cisco IOS Software Layer 2 Tunneling Protocol (L2TP) Denial of Service Vulnerability

Advisory ID: [cisco-sa-20080924-l2tp](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml>

## Revision 1.1

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

A vulnerability exists in the Cisco IOS software implementation of Layer 2 Tunneling Protocol (L2TP), which affects limited Cisco IOS software releases.

Several features enable the L2TP mgmt daemon process within Cisco IOS software, including but not limited to Layer 2 virtual private networks (L2VPN), Layer 2 Tunnel Protocol Version 3 (L2TPv3), Stack Group Bidding Protocol (SGBP) and Cisco Virtual Private Dial-Up Networks (VPDN). Once this process is enabled the device is vulnerable.

This vulnerability will result in a reload of the device when processing a specially crafted L2TP packet.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml>.

**Note:** 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-vpn.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>

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

## ☐ Affected Products

All devices running affected versions of 12.2 or 12.4 Cisco IOS system software and that have a vulnerable configuration are affected by this vulnerability.

## ☐ Vulnerable Products

To determine if a device is vulnerable, first confirm that the device is running an affected version of 12.2 or 12.4 Cisco IOS system software. Then check for the process **L2TP mgmt daemon** running on the device.

To determine the software version 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 Software 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 in the document entitled "White Paper: Cisco IOS Reference Guide," which is available at <http://www.cisco.com/warp/public/620/1.html>

To check if the process **L2TP mgmt daemon** is running on a device, log into the command line interface (CLI) and issue the command **show processes | include L2TP** . (NOTE: The command is case sensitive.) If the output returns a line with the process name **L2TP mgmt daemon**, the device is vulnerable. The following example shows a device running the **L2TP mgmt daemon** process:

```
Router#show processes | include L2TP
 158 Mwe 62590FE4          4          3      133322900/24000  0 L2TP mgmt
Router#
```

The L2TP mgmt daemon is started by several different types of configurations that may be deployed in networks that leverage the L2TP protocol. If any of the following commands appear within a device's configuration, **show running-config**, then the device will have started the L2TP mgmt daemon and is vulnerable.

- Device is configured with Virtual Private Dial-Up Networks (VPDN).  
The command **vpdn enable** will appear in the device configuration.
- Device is configured for L2TP or L2TPv3 Client-Initiated VPDN Tunneling.  
The command **pseudowire peer-ip-address vcid pw-class pw-class-name** " appears in the device configuration.
- Device is configured with Stack Group Bidding Protocol (SGBP).  
The command **sgbp group group-name** will appear in the device configuration.
- A L2TP signaling template has been defined.  
The command **l2tp-class l2tp-class name** will appear in the device configuration.
- Devices configured for Layer 2 Tunnel Protocol Version 3  
The commands **pseudowire-class pseudowire-class name** and a successfully applied interface **xconnect** command will appear in the device configuration.

## ☐ Products Confirmed Not Vulnerable

- Devices that are running Cisco IOS versions that are not explicitly listed in the software table below as vulnerable, are not affected.

- Cisco IOS XR is not affected.
- Cisco IOS XE is not affected.

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

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

## ▣ Details

Documented in [RFC2661](#), L2TP and [RFC3931](#), L2TPv3 are protocols for tunneling network traffic between two peers over an existing network.

A device running affected 12.2 and 12.4 versions of Cisco IOS and that has the L2TP mgmt daemon process running will reload when processing a specially crafted L2TP packet.

Several features leverage the L2TP protocol and start the L2TP mgmt daemon within Cisco IOS. These features have been outlined in this advisory under the Vulnerable Products section.

This vulnerability is documented in Cisco bug ID [CSCsh48879](#) ([registered](#) customers only) and Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3813 has been assigned to this vulnerability.

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

## ▣ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability 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>.

**[CSCsh48879](#) ( [registered](#) customers only) - Crafted L2TP packet triggers a device reload.**

Calculate the environmental score of <a href="#">CSCsh48879</a>					
CVSS Base Score - <b>7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - <b>6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## ▣ Impact

Successful exploitation of the vulnerability will result in a reload of the device. Repeated exploitation may result in an extended denial of service (DoS) condition.

[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 Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases		

<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	Not Vulnerable	
12.2IXB	Not Vulnerable	
12.2IXC	Not Vulnerable	
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	Not Vulnerable	
12.2SB	Not Vulnerable	
12.2SBC	Not Vulnerable	
12.2SCA	Not Vulnerable	
12.2SE	Note: Releases prior to 12.2(37)SE are not vulnerable. First fixed in 12.2(44)SE	12.2(46)SE
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	Note: Releases prior to 12.2(37)SG are not vulnerable. First Fixed in 12.2(44)SG	12.2(46)SG1
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SRA	Not Vulnerable	
12.2SRB	12.2(33)SRB1	12.2(33)SRB4
12.2SRC	Not Vulnerable	
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
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	Not Vulnerable	
12.2SXF	Not Vulnerable	
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	Not Vulnerable	
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.3 based releases		
<b>Affected 12.4-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	Not Vulnerable	
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	Note: Releases prior to 12.4(11)MR are not vulnerable. First fixed in 12.4(16)MR	12.4(19)MR
12.4SW	12.4(11)SW3	12.4(15)SW2; Available on 28-SEP-08
12.4T	Note: Releases prior to 12.4(11)T are not vulnerable. First fixed in 12.4(15)T	12.4(15)T7
12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	
12.4XC	Not Vulnerable	

12.4XD	Not Vulnerable	
12.4XE	Not Vulnerable	
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Vulnerable; contact TAC	
12.4XW	12.4(11)XW1	12.4(11)XW9
12.4XY	Not Vulnerable	
12.4XZ	Not Vulnerable	
12.4YA	Not Vulnerable	

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

## ☐ Workarounds

The following workarounds have been identified for this vulnerability.

**Note:** L2TP implementations will need to allow UDP 1701, from trusted addresses to infrastructure addresses. This does not provide for a full mitigation as the source addresses may be spoofed.

**Note:** L2TPv3 over IP only implementations need to deny all UDP 1701 from anywhere to the infrastructure addresses.

- Infrastructure Access Control Lists

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities. The iACL example below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:

```

!--- Permit L2TP UDP 1701 packets from all trusted
!--- sources destined to infrastructure addresses.
!--- NOTE: This does not prevent spoofed attacks.
!---           To be a full mitigation, no trusted source
!---           addresses should be listed.
!---           Omit this line if using a L2TPv3 over IP implementation

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES MASK
          INFRASTRUCTURE_ADDRESSES MASK eq 1701

!--- Deny L2TP UDP 1701 packets from all
!--- sources destined to infrastructure addresses.

access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 1701

!--- If using a L2TPv3 over IP implementation ensure to allow L2TPv3

access-list 150 permit 115 <source_ip_address and mask>
          <destination_ip_address and 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

!--- Apply access-list to all interfaces (only one example shown)

interface serial 2/0
ip access-group 150 in

```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:  
[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_white\\_paper09186a00801a1a55.s](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.s)

- Control Plane Policing

Control Plane Policing (CoPP) can be used to block L2TP access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP which will protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Deny all trusted source L2TP UDP traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will not be policed by the CoPP feature.

!--- NOTE: This does not prevent spoofed attacks.
!---           To be a full mitigation, no trusted source
!---           addresses should be listed.
!---           Omit this line if using an L2TPv3 over IP implementation

access-list 111 deny udp TRUSTED_SOURCE_ADDRESSES MASK
                INFRASTRUCTURE_ADDRESSES MASK eq 1701

!--- Permit all L2TP UDP 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 INFRASTRUCTURE_ADDRESSES MASK eq 1701

!--- If using an L2TPv3 over IP implementation ensure not to drop L2TPv

access-list 111 deny 115 <source_ip_address and mask>
                <destination_ip_address and mask>

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!--- 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-l2tp-class
match access-group 111

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-l2tp-traffic
class drop-l2tp-class
drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device
```

```
control-plane
service-policy input drop-l2tp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS trains:

```
policy-map drop-l2tp-traffic
class drop-l2tp-class
police 32000 1500 1500 conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature is available at the following link: [http://www.cisco.com/web/about/security/intelligence/coppwp\\_gs.html](http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html)

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory: <http://www.cisco.com/warp/public/707/cisco-amb-20080924-l2tp.shtml>.

[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 or 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 found by Cisco through internal testing.

[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-l2tp.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-teams@first.org](mailto:first-teams@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 1.1	2009-April-16	Removed references to the combined software table, as it is now outdated
Revision 1.0	2008-September-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.](#)