

Cisco Security Advisory: Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability

Advisory ID: cisco-sa-20080326-pptp

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml>

Revision 1.2

Last Updated 2008 July 03 1430 UTC (GMT)

For Public Release 2008 March 26 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](#)

Summary

Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted.

Cisco has made free software available to address these vulnerabilities for affected customers.

There are no workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml>.

Note: The March 26, 2008 publication includes five security advisories. The advisories all address vulnerabilities in Cisco's IOS software. Each advisory lists the releases that correct the vulnerability described in the advisory, and also lists the releases that correct the vulnerabilities in the other five advisories.

Individual publication links are listed below:

- Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml>
- Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>
- Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>
- Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml>

- Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak
<http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>

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

☐ Affected Products

Devices that are running certain Cisco IOS versions prior to 12.3 with VPDN enabled may be affected by these vulnerabilities.

☐ Vulnerable Products

Devices that are running affected versions of Cisco IOS with VPDN enabled and are configured to accept termination of PPTP sessions are vulnerable.

To determine whether VPDN is enabled on your device, log in to the device and issue the command-line interface (CLI) command **show running-config**. If the output contains **vpdn enable** along with a **vpdn-group <name>** command, VPDN is enabled on the device. The device will accept termination of PPTP sessions if the command **protocol any** or **protocol pptp** is defined under the **vpdn-group <name>** command. The following example shows a device that is running VPDN and will accept termination of PPTP sessions:

```
Router#show running-config
Building configuration...

!
!--- Output truncated.
!

vpdn enable

!

vpdn-group test_only
! Default PPTP VPDN group
  accept-dialin
  protocol pptp
  virtual-template 1

!
```

!---Remaining output truncated.

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 release 12.2(7):

```
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-IS-M), Version 12.2(7),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 15-Jan-02 18:31 by pwade
Image text-base: 0x600089C0, data-base: 0x613A6000
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

☐ Products Confirmed Not Vulnerable

Devices that are running Cisco IOS versions 12.3 and later are not affected by these vulnerabilities. Devices that are explicitly configured for VPDN protocols other than PPTP are not affected.

Devices that are running Cisco IOS versions prior to 12.3 and do not have VPDN enabled are not affected by these vulnerabilities.

Cisco IOS XR is not affected by these vulnerabilities.

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

☐ Details

VPDNs securely carry private data over a public network, allowing remote users to access a private network over a shared infrastructure such as the Internet. VPDNs maintain the same security and management policies as a private network, while providing a cost-effective method for point-to-point connections between remote users and a central network.

PPTP is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPDN across TCP/IP-based data networks. PPTP supports on-demand, multiprotocol, virtual private networking over public networks, such as the Internet.

Details regarding the two known vulnerabilities in Cisco IOS devices that are running affected versions of system software follow:

- **Memory Leak due to PPTP Session Termination**

Upon completion of a PPTP session, memory is leaked from the processor memory on the terminating device. This is shown in the output of **show process memory** under the **Dead** process. The **Dead** process is not a real process. Its function is to account for the memory that is allocated under the context of another process which has terminated, in this case PPTP. When the administrator is logged into the device, if the device is under exploitation, the **Holding** entry of the **Dead** process under the **show process memory** command will be increasing. Following is an example showing a device that is holding **Dead** memory:

```
Router#show process memory
Total: 199718560, Used: 11147828, Free: 188570732
  PID TTY   Allocated      Freed   Holding
Getbufs   Retbufs Process
   0   0     99812        1848   8415816
0                0 *Init*
   0   0         444    778840       444
0                0 *Sched*
   0   0  17481700    4930848   819672
180908                0 *Dead*
   1   0         284         284    3828
0                0 Load Meter
```

!--- Output truncated.

The CLI command **show memory dead** allows administrators to examine the contents of **Dead**. The output will display many occurrences of PPTP in the output if the PPTP process is causing the leak. The following example shows the dead memory for a device that has been exploited by the vulnerability

```
Router#show memory dead
                Head    Total(b)    Used(b)    Free
(b)  Lowest(b)  Largest(b)
Processor  6225FF40  224002240  11906736
```

```

212095504    212082872    212084464
           I/O    20000000    33554440    994136
32560304    32560304    32560252
           I/O-2    F800000    8388616    1020632
7367984    7367984    7367932

```

Processor memory

```

Address      Bytes      Prev      Next Ref      PrevF
NextF Alloc PC  what
62275DC8 0000000048 62275D68 62275E24 001  -----
----- 60654230 PPTP create idb
62275E24 0000000052 62275DC8 62275E84 001  -----
----- 60654230 PPTP create idb
62275E84 0000000052 62275E24 62275EE4 001  -----
----- 60654230 PPTP create idb
.....

```

!--- remaining output truncated.

This vulnerability is documented in Cisco bug ID [CSCsj58566](#) (**registered customers only**) and Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1151 has been assigned to this vulnerability.

- **Virtual Access Interfaces Are Not Re-used**

Upon completion of a PPTP session, affected devices do not remove the virtual access interface that is associated with the PPTP session and do not reuse the interfaces in any future connections.

This situation can result in an exhaustion of the interface descriptor block (IDB) limit, which will prevent any new interfaces being created within Cisco IOS, effectively blocking all new VPDN connections, even though the router may still have enough processor memory to remain up and running. A reload of the device is required to remove the interfaces.

An IDB is a Cisco IOS internal data structure that contains information such as the IP address, interface state, and packet statistics. Cisco IOS software maintains one IDB for each interface present on a platform and one IDB for each subinterface.

Further documentation on Cisco IOS IDBs can be found at: <http://www.cisco.com/en/US/>

products/sw/iosswrel/ps1835/products_tech_note09186a0080094322.shtml

This vulnerability is documented in Cisco bug ID [CSCdv59309](#) ([registered customers only](#)) and Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1150 has been assigned to this vulnerability.

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

☐ Vulnerability Scoring Details

Cisco is providing 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.

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

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

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>.

[CSCsj58566](#) ([registered customers only](#)) - Memory Leak due to PPTP Session Termination

Calculate the environmental score of [CSCsj58566](#)

CVSS Base Score - **7.1**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete

CVSS Temporal Score - **5.9**

Exploitability	Remediation Level	Report Confidence
----------------	-------------------	-------------------

Functional	Official-Fix	Confirmed
------------	--------------	-----------

CSCdv59309 (registered customers only) - Virtual Access Interfaces Are Not Re-used

Calculate the environmental score of CSCdv59309

CVSS Base Score - 4.3

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Partial

CVSS Temporal Score - 3.6

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

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

[-] Impact

Successful exploitation of the vulnerability may result in a memory leak of processor memory or consumption of all available IDBs on the device. With continued exploitation, the device will deplete its processor memory or reach an IDB limit. Both impacts would result in a denial of service condition for the device.

[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
12.0	Not Vulnerable	
12.0DA	Not Vulnerable	
12.0DB	Not Vulnerable	
12.0DC	Not Vulnerable	
12.0S	Not Vulnerable	
12.0SC	Not Vulnerable	
12.0SL	Not Vulnerable	
12.0SP	Not Vulnerable	
12.0ST	Not Vulnerable	

12.0SX	Not Vulnerable
12.0SY	Not Vulnerable
12.0SZ	Not Vulnerable
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	Releases prior to 12.0(7)XE2 are vulnerable, release 12.0(7)XE2 and later are 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	
12.0XV	Not Vulnerable	
12.0XW	Not Vulnerable	
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
12.1	Not Vulnerable	
12.1AA	Not Vulnerable	

12.1AX	Not Vulnerable	
12.1AY	Releases prior to 12.1(22)AY1 are vulnerable, release 12.1(22)AY1 and later are not vulnerable;	12.1(22)EA11
12.1AZ	Not Vulnerable	
12.1CX	Not Vulnerable	
12.1DA	Not Vulnerable	
12.1DB	Not Vulnerable	
12.1DC	Vulnerable; first fixed in 12.2B	12.4(18a)
12.1E	Vulnerable; contact TAC	
12.1EA	Releases prior to 12.1(11)EA1 are vulnerable, release 12.1(11)EA1 and later are not vulnerable;	12.1(22)EA11
12.1EB	Not Vulnerable	
12.1EC	Vulnerable; first fixed in 12.2BC	12.3(23)BC1
12.1EO	Not Vulnerable	

12.1EU	Not Vulnerable	
12.1EV	Not Vulnerable	
12.1EW	Not Vulnerable	
12.1EX	Vulnerable; contact TAC	
12.1EY	Not Vulnerable	
12.1EZ	Vulnerable; contact TAC	
12.1GA	Not Vulnerable	
12.1GB	Not Vulnerable	
12.1T	Vulnerable; migrate to any release in 12.3	12.3(26)
12.1XA	Not Vulnerable	
12.1XB	Not Vulnerable	
12.1XC	Not Vulnerable	
12.1XD	Not Vulnerable	
12.1XE	Not Vulnerable	
12.1XF	Not Vulnerable	

12.1XG	Not Vulnerable	
12.1XH	Not Vulnerable	
12.1XI	Not Vulnerable	
12.1XJ	Vulnerable; first fixed in 12.2T	12.3(26)
12.1XK	Not Vulnerable	
12.1XL	Vulnerable; first fixed in 12.2T	12.3(26)
12.1XM	Vulnerable; first fixed in 12.2T	12.3(26)
12.1XN	Not Vulnerable	
12.1XO	Not Vulnerable	
12.1XP	Vulnerable; first fixed in 12.2T	12.3(26)
12.1XQ	Vulnerable; first fixed in 12.2T	12.3(26)
12.1XR	Vulnerable; first fixed in 12.2T	12.3(26)
12.1XS	Vulnerable; migrate to any release in 12.3	12.3(26)
12.1XT	Vulnerable; first fixed in 12.2T	12.3(26)
12.1XU	Not Vulnerable	

12.1XV	Vulnerable; first fixed in 12.2XB	12.3(26)
12.1XW	Not Vulnerable	
12.1XX	Not Vulnerable	
12.1XY	Vulnerable; migrate to any release in 12.3	12.3(26)
12.1XZ	Not Vulnerable	
12.1YA	Vulnerable; first fixed in 12.2T	12.3(26)
12.1YB	Vulnerable; first fixed in 12.2T	12.3(26)
12.1YC	Vulnerable; first fixed in 12.2T	12.3(26)
12.1YD	Vulnerable; first fixed in 12.2T	12.3(26)
12.1YE	Releases prior to 12.1(5)YE6 are vulnerable, release 12.1(5)YE6 and later are not vulnerable; first fixed in 12.2T	12.3(26)
12.1YF	Vulnerable; first fixed in 12.2T	12.3(26)
12.1YG	Not Vulnerable	
12.1YH	Not Vulnerable	

12.1YI	Vulnerable; first fixed in 12.2T	12.3(26)
12.1YJ	Not Vulnerable	
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
12.2	Vulnerable; migrate to any release in 12.3	12.3(26)
12.2B	12.2(4)B5	12.4(18a)
12.2BC	12.2(15)BC1e 12.2(15)BC2d 12.2(8)BC1	12.3(23)BC1
12.2BW	12.2(4)BW1 12.2(4)BW1a	12.3(26)
12.2BY	12.2(8)BY	12.4(18a)
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Not Vulnerable	
12.2DA	Vulnerable; contact TAC	

12.2DD	Vulnerable; first fixed in 12.2B	12.4(18a)
12.2DX	Vulnerable; first fixed in 12.2B	12.4(18a)
12.2EU	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	
12.2IXA	Not Vulnerable	
12.2IXB	Not Vulnerable	
12.2IXC	Not Vulnerable	
12.2IXD	Not Vulnerable	
12.2IXE	Not Vulnerable	

12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	
12.2S	Releases prior to 12.2(18)S are vulnerable, release 12.2(18)S and later are not vulnerable; migrate to any release in 12.2SRC	12.2(25)S15
12.2SB	Not Vulnerable	
12.2SBC	Not Vulnerable	
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	Not Vulnerable	
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SRA	Not Vulnerable	
12.2SRB	Not Vulnerable	
12.2SRC	Not Vulnerable	
12.2SU	Vulnerable; migrate to any release in 12.3T	12.4(18a)
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	

12.2SVD	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Releases prior to 12.2(17a)SX are vulnerable, release 12.2(17a)SX and later are not vulnerable; migrate to any release in 12.2SXF	12.2(18)SXF13
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	Vulnerable; migrate to any release in 12.2SXB	12.2(18)SXF13
12.2SZ	Vulnerable; migrate to any release in 12.2SRC	12.2(25)S15 12.2(31)SB11 12.2(33)SRC

12.2T	12.2(15)T4e 12.2(8)T	12.3(26)
12.2TPC	Not Vulnerable	
12.2UZ	Not Vulnerable	
12.2XA	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XB	12.2(2)XB5	12.3(26)
12.2XC	Vulnerable; migrate to any release in 12.3T	12.4(18a)
12.2XD	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XE	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XF	Vulnerable; first fixed in 12.2BC	12.3(23)BC1
12.2XG	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XH	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XI	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XJ	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XK	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XL	Not Vulnerable	

12.2XM	Not Vulnerable	
12.2XN	Not Vulnerable	
12.2XO	Not Vulnerable	
12.2XQ	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XR	Not Vulnerable	
12.2XS	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XT	Vulnerable; first fixed in 12.2T	12.3(26)
12.2XU	Vulnerable; migrate to any release in 12.3	12.3(26)
12.2XV	Vulnerable; migrate to any release in 12.3	12.3(26)
12.2XW	Not Vulnerable	
12.2YA	Not Vulnerable	
12.2YB	Not Vulnerable	
12.2YC	Vulnerable; first fixed in 12.2T	12.3(26)
12.2YD	Not Vulnerable	

12.2YE	Vulnerable; migrate to any release in 12.2SRC	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
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	Vulnerable; migrate to any release in 12.2SXB	12.2(18)SXF13
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	Vulnerable; migrate to any release in 12.3T	12.4(18a)
12.2YY	Not Vulnerable	
12.2YZ	Vulnerable; migrate to any release in 12.2SRC	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2ZA	Vulnerable; migrate to any release in 12.2SXB	12.2(18)SXF13
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	
12.2ZY	Not Vulnerable	
Affected 12.3-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.4 based releases		

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

☐ Workarounds

There are no workarounds for these vulnerabilities. Cisco recommends upgrading to the fixed version of Cisco IOS.

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

☐ Obtaining Fixed Software

Cisco will make free software available to address these vulnerabilities for affected customers. This advisory will be updated as fixed software becomes available. 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/public/sw-license-agreement.html> , or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "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 agreement 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 who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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

Have your product serial number available and give the URL of this notice as evidence of your 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 special 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.

We would like to thank Martin Kluge of Elxsi Security for reporting these vulnerabilities to us. We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist with security vulnerability reports against Cisco products.

[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-20080206-pptp.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
- first-teams@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

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	2008-June-27	Updated Summary to remove link and verbiage.
Revision 1.1	2008-March-29	Updated Software Table for 12.0S, 12.0SY, 12.0SX and 12.0SZ due to new information on advisory ID cisco-sa-20080326-IPv4IPv6 , the March 26th advisory on IPv4IPv6 Dual Stack Routers.
Revision 1.0	2008-March-26	Initial public release

☐ 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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

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)



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

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)