

# Cisco Security Advisory: Cisco IOS cTCP Denial of Service Vulnerability

Advisory ID: cisco-sa-20090325-ctcp

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>

## Revision 1.0

For Public Release 2009 March 25 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 series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPsec NAT traversal (NAT-T) feature can be used as an alternative.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>.

**Note:** The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The

following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-bundle.shtml>

Individual publication links are listed below:

- Cisco IOS cTCP Denial of Service Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>
- Cisco IOS Software Multiple Features IP Sockets Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>
- Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>
- Cisco IOS Software Secure Copy Privilege Escalation Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>
- Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml>
- Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml>
- Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>
- Cisco IOS Software WebVPN and SSLVPN Vulnerabilities  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

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

## ☐ Affected Products

### ☐ Vulnerable Products

Cisco IOS devices running versions 12.4(9)T or later and configured for Cisco Tunneling Control Protocol (cTCP) encapsulation for EZVPN server are vulnerable.

**Note:** The cTCP encapsulation feature was introduced in Cisco IOS version 12.4(9)T. The cTCP encapsulation feature is disabled by default. Cisco IOS devices configured for EZVPN client are not affected by this vulnerability. Only devices configured as EZVPN servers are vulnerable.

To configure the cTCP encapsulation feature for Easy VPN, use the **crypto tcp** command in global configuration mode. You can optionally specify the port number that the device will listen to with the **crypto tcp port <port>** command. Up to ten numbers can be configured and the port value can be from 1 through 65535. If the port keyword is not configured, the default port number is 10000. In the following example, the Cisco IOS device is configured to listen for cTCP messages on port 10000.

```
crypto tcp port 10000
```

**Note:** The port keyword is configured only on the Cisco IOS device acting as an EZVPN server.

To determine the version of the Cisco IOS 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 running Cisco IOS Software release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOF
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih
```

<output truncated>

The next example shows a product running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Versi
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 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 IOS devices that are not configured for cTCP are not affected by this vulnerability. The Cisco ASA and Cisco VPN 3000 series concentrators are not vulnerable. Cisco IOS devices configured as EZVPN clients are not affected by this vulnerability. The Cisco VPN Client is not vulnerable. Cisco IOS-XR and Cisco IOS-XE software are not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

## ▣ Details

The Cisco Tunneling Control Protocol (cTCP) feature is used by Easy VPN remote device operating in an environment in which standard IPsec does not function transparently without modification to existing firewall rules. The cTCP traffic is actually TCP traffic. Cisco IOS cTCP packets are Internet Key Exchange (IKE) or Encapsulating Security Payload (ESP) packets that are being transmitted over TCP.

A vulnerability exists where a series of TCP packets may cause a Cisco IOS device that is configured as an Easy VPN server with the cTCP encapsulation feature to run out of memory. This vulnerability is documented in Cisco Bug IDs [CSCsr16693](#) ( [registered](#) customers only) and [CSCsu21828](#) ( [registered](#) customers only) ; and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0635.

## ▣ 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>.

<b>CSCsr16693 - cTCP server may crash when processing a series of TCP packets</b>					
<b>Calculate the environmental score of <a href="#">CSCsr16693</a></b>					
<b>CVSS Base Score - 7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
<b>CVSS Temporal Score - 6.4</b>					
Exploitability		Remediation Level		Report Confidence	

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

<b>CSCsu21828 - Cisco IOS Device may crash with cTCP enabled</b>					
<b>Calculate the environmental score of <a href="#">CSCsu21828</a></b>					
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 this vulnerability may cause the affected device to run out of memory. Repeated exploitation will result in a 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>
There are no affected 12.2 based releases		
<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	
12.4JDA	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	Not Vulnerable	
12.4T	12.4(20)T2  12.4(15)T9; Available on 29- APR-2009	12.4(22)T1  12.4(15)T9; Available on 29- APR-2009
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	Not Vulnerable	
12.4XK	Not Vulnerable	

12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	Not Vulnerable	
12.4XZ	12.4(15)XZ2	12.4(15)XZ2
12.4YA	12.4(20)YA2	12.4(20)YA3
12.4YB	Not Vulnerable	
12.4YD	Not Vulnerable	

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

## ☐ Workarounds

No workarounds are available.

As an alternative, the IPsec NAT traversal (NAT-T) feature can be used. The IPsec NAT-T feature introduces support for IP Security (IPsec) traffic to travel through Network Address Translation (NAT) or Port Address Translation (PAT) points in the network by addressing many known incompatibilities between NAT and IPsec.

**Note:** The NAT-T feature was introduced in Cisco IOS version 12.2(13)T.

NAT Traversal is a feature that is auto detected by VPN devices. There are no configuration steps for a router running Cisco IOS Release 12.2(13)T and later. If both VPN devices are NAT-T capable, NAT Traversal is auto-detected and auto-negotiated.

**Note:** When you enable NAT-T, the Cisco IOS device automatically opens UDP port 4500 on all IPsec enabled interfaces.

**Caution:** Be aware that you may need to enable IPsec over UDP on Cisco VPN software clients to support NAT-T. Additionally, you may need to change firewall rules to allow UDP port 500 for Internet Key Exchange (IKE) and UDP port 4500 for NAT-T.

For more information about NAT-T, refer to the white paper at:

[http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec\\_ipsec\\_nat\\_transp.html](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_ipsec_nat_transp.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, which is available at the following link:

## ☐ **Obtaining Fixed Software**

Cisco has released free software updates that address this vulnerability. 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/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) 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 during the resolution of a technical support service request.

[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-20090325-ctcp.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.

## ☐ Revision History

Revision 1.0	2009-March-25	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](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)

☐

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

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

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