

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS cTCP Denial of Service Vulnerability

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

Revision 1.0

For Public Release 2009 March 25 1600 UTC (GMT)

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

Contents

[Cisco Response](#)
[Device-Specific Mitigation and Identification](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Cisco IOS cTCP Denial of Service Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

The Cisco IOS Easy VPN Cisco Tunneling Control Protocol (cTCP) encapsulation feature contains a vulnerability in processing malicious cTCP packets. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may cause denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through cTCP packets, which use TCP port 10000 as the default port. An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2009-0635.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for this vulnerability. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network. This section of the document provides an overview of these techniques.

One component of this vulnerability, **cTCP server may crash when processing a series of TCP packets** (Cisco bug ID CSCsr16693) can be mitigated by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using TCP Intercept.

Cisco IOS NetFlow can provide visibility into network-based exploitation attempts using flow records.

Cisco IOS Software, Cisco ASA appliances, and Cisco PIX security appliances can provide visibility through counter values displayed in the output from **show** commands.

Risk Management

Organizations are advised to follow their standard risk evaluation and mitigation processes to determine the potential impact of this vulnerability. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk-based triage capability for their information security teams. [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#) can help organizations develop repeatable security evaluation and response processes.

Device-Specific Mitigation and Identification

Caution: The effectiveness of any mitigation technique depends on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

Specific information about mitigation and identification is available for these devices:

- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)

Cisco IOS NetFlow

Identification: Traffic Flow Identification Using NetFlow Records

Administrators can configure Cisco IOS NetFlow on Cisco IOS routers and switches to aid in the identification of traffic flows that may be attempts to exploit this vulnerability. Administrators are advised to investigate flows to determine whether they are attempts to exploit this vulnerability or whether they are legitimate traffic flows. The attack vector for exploitation is through cTCP packets using TCP port 10000 (default port).

```
router#show ip cache flow
IP packet size distribution (53684999 total packets):
```

```

1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  48
.000 .331 .224 .088 .087 .022 .074 .028 .001 .000 .004 .002 .000 .000 .00

```

```

512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
.001 .000 .001 .032 .092 .000 .000 .000 .000 .000 .000

```

```

IP Flow Switching Cache, 4456704 bytes
50 active, 65486 inactive, 5539379 added
181719720 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds

```

```

IP Sub Flow Cache, 533256 bytes
50 active, 16334 inactive, 5539379 added, 5539379 added to flow
0 alloc failures, 2161 force free
1 chunk, 6 chunks added
last clearing of statistics never

```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Se /Flow
TCP-Telnet	5813	0.0	3	50	0.0	2.2	29.1
TCP-FTP	2968	0.0	1	49	0.0	1.6	45.4
TCP-FTPD	1826	0.0	70	843	0.0	0.6	39.2
TCP-WWW	61898	0.0	48	671	1.7	14.4	31.0
TCP-SMTP	2199	0.0	1	96	0.0	0.2	42.5
TCP-X	1719	0.0	1	42	0.0	0.0	43.6
TCP-BGP	1661	0.0	1	42	0.0	0.0	42.7
TCP-NNTP	1693	0.0	1	42	0.0	0.0	42.9
TCP-Frag	1	0.0	1	40	0.0	0.0	60.2
TCP-other	4007547	2.3	6	300	14.2	0.9	25.4
UDP-DNS	84067	0.0	4	68	0.2	26.1	48.1
UDP-NTP	138637	0.0	1	76	0.1	8.2	57.2
UDP-TFTP	4	0.0	1	28	0.0	0.0	60.3
UDP-other	529788	0.3	43	133	13.1	20.7	51.3
ICMP	491126	0.2	1	80	0.4	2.1	60.0
IGMP	71601	0.0	2	39	0.0	59.0	42.2
IPINIP	1	0.0	4	105	0.0	24.8	60.5
IPv6INIP	1	0.0	4	145	0.0	24.5	60.8
IP-other	136782	0.0	10	92	0.7	95.6	14.5
Total:	5539332	3.1	9	239	30.8	6.7	32.1

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pk
Gi0/0	192.168.208.127	Gi0/0	192.168.104.132	06	94AD	1A29	
Gi0/0	192.168.10.21	Gi0/1	192.168.60.1	06	081F	2710	
Gi0/0	192.168.10.10	Gi0/1	192.168.60.71	06	081E	2710	
Gi0/0	192.168.10.12	Gi0/1	192.168.60.21	06	081D	2710	
Gi0/0	192.168.10.31	Gi0/1	192.168.60.10	06	081C	2710	
Gi0/0	192.168.10.11	Gi0/1	192.168.60.16	06	081B	2710	
Gi0/0	192.168.10.17	Gi0/1	192.168.60.100	06	0824	2710	
Gi0/0	192.168.10.1	Gi0/1	192.168.60.1	11	010A	0053	2

```

router#

```

In the preceding example, there are multiple flows for **cTCP** on **TCP** port **10000** (hex value **2710**).

This traffic is sent to addresses within the 192.168.60.0/24 address block, which is used by affected devices. The packets in these flows may indicate an attempt to exploit this vulnerability. Administrators are advised to compare these flows to baseline utilization for cTCP traffic sent on TCP port 10000 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for cTCP packets on TCP port 10000 (hex value 2710), the **show ip cache flow | include SrcIf_06_.*2710** command will display the related TCP NetFlow records as shown here:

TCP Flows

```
router#show ip cache flow | include SrcIf|_06_.*2710
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  P
Gi0/0     192.168.10.1      Gi0/1      192.168.60.1     06 0B8F 2710
Gi0/0     192.168.10.1      Gi0/1      192.168.60.1     06 0B8E 2710
Gi0/0     192.168.10.1      Gi0/1      192.168.60.1     06 0B8D 2710
Gi0/0     192.168.10.1      Gi0/1      192.168.60.1     06 0B8C 2710
Gi0/0     192.168.10.1      Gi0/1      192.168.60.1     06 0B8B 2710
router#
```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Embryonic Connection Limiting with TCP Intercept

TCP Intercept can mitigate one component of the vulnerability: **cTCP server may crash when processing a series of TCP packets** (Cisco bug ID CSCsr16693) TCP Intercept will force connecting source endpoints to validate themselves through the use of SYN cookies. Administrator can configure this form of protection by using static NAT or static identity NAT for ASA, PIX, and FWSM firewalls. In addition, the ASA firewall and the Cisco PIX 500 Series Security Appliance may be configured to use TCP Intercept through the use of the Modular Policy Framework (MPF).

Additional information is available regarding on [Static NAT](#), [Static Identity NAT](#) and the [Modular Policy Framework](#).

In the following example, an embryonic connection limit of one will be set. This limit will, in effect, force simultaneous TCP connections to be validated using SYN cookies. The following commands will set an embryonic connection limit of one for connections to TCP port 10000 for hosts in the 192.168.60.0/24 subnet. It is possible to use the MPF configuration method to set an embryonic connection timeout. The default is 30 seconds. In the following example, the policy is applied globally to all interfaces.

```
!
!-- Configure an access list that will be used to match on default cTCP traf.
!-- to affected devices
!

access-list TCP-Intercept-ACL extended permit tcp any 192.168.60.0 255.255.2

!
!-- Configure a class that uses the above-configured access list
!-- to match TCP packets that are destined to the port used by cTCP
!

class-map TCP-Intercept-Class
 match access-list TCP-Intercept-ACL

!
!-- Add the above-configured "TCP-Intercept-Class" that matches
!-- TCP packets that are destined to the default port that
!-- is used by the cTCP feature to the default
!-- policy "global_policy" and use it to inspect
!-- TCP traffic that transits the firewall
!

policy-map global_policy
```

```

!
!-- For the TCP-Intercept-Class, set the embryonic connection maximum to 1,
!-- which will trigger SYN cookies when there is more than one simultaneous
!

class TCP-Intercept-Class
  set connection embryonic-conn-max 1

!
!-- By default, the policy "global_policy" is applied
!-- globally, which results in the inspection of
!-- traffic that enters the firewall from all interfaces
!

service-policy global_policy global

```

Additional information about connection limits is in the [Preventing Network Attacks](#) section of the Cisco Security Appliance Command Line Configuration Guide.

Identification: Threat Detection Statistics

TCP Intercept Statistics

Beginning with ASA and PIX version 8.0(4), TCP Intercept threat detection statistics are enabled by the **threat-detection statistics tcp-intercept** command documented in the [Cisco Security Appliance Command Reference](#). These statistics reflect mitigation performed as a result of embryonic connection limits that are configured by static NAT, static identity NAT or by using the Modular Policy Framework (MPF). In the following example, the **show threat-detection statistics top tcp-intercept** command provides information on the top ten protected servers under attack.

```

ASA#show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins      Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP>
-----
 1   192.168.128.26:10000 outside 12 109 22744 <various> Last: 192.168.60.10
 2   192.168.1.7:8200 outside 0 0 4 198.18.80.77 (50 secs ago)
 3   192.168.206.5:80 outside 0 0 2 192.168.180.202 (3 mins ago)
 4   192.168.210.13:80 outside 0 0 2 192.168.180.202 (3 mins ago)
 5   192.168.206.5:443 outside 0 0 2 192.168.180.202 (3 mins ago)
 6   192.168.206.5:21 outside 0 0 2 192.168.180.202 (3 mins ago)
 7   192.168.206.5:22 outside 0 0 2 192.168.180.202 (3 mins ago)
 8   192.168.206.5:5900 outside 0 0 2 192.168.180.202 (3 mins ago)
 9   192.168.206.40:80 outside 0 0 2 192.168.180.202 (3 mins ago)
10   192.168.154.43:80 outside 0 0 2 192.168.180.202 (3 mins ago)

```

In the preceding example, **22744 cTCP packets** on TCP port 10000 that were received inbound on the interface outside have been dropped. The average rate of attack during the monitoring window was **12** packets per second, and **109** packets per second is the attack rate in the current sampling interval.

Information about configuring threat protection for the Cisco ASA 5500 Series Adaptive Security Appliance is in [Configuring and Viewing Threat Statistics](#).

Additional Information

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.

Revision History

Revision 1.0	2009-Mar-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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Related Information

- [Cisco Applied Mitigation Bulletins](#)
- [Cisco Guide to Harden Cisco IOS Devices](#)
- [Cisco Security Center](#)
- [Understanding Cross-Site Scripting \(XSS\) Threat Vectors](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [NetFlow Performance Analysis](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [TTL Expiry Attack Identification and Mitigation](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Countermeasures for the Malicious Use of IPv6 Type 0 Routing Headers](#)
- [Understanding Control Plane Protection](#)
- [Securing Tool Command Language on Cisco IOS](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS 6.x Signature Downloads](#)
- [Cisco IPS Signature Search Page](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)
- [Cisco Security Agent](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#)

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)

Send

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.](#)