

Cisco Security Advisory: Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability

Advisory ID: cisco-sa-20090325-tcp

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

Revision 1.2

Last Updated 2009 July 07 2030 UTC (GMT)

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

Cisco IOS[®] Software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets

can cause the vulnerable device to reload.

Cisco has released free software updates that address this vulnerability.

Several mitigation strategies are outlined in the workarounds section of this advisory.

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

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

Devices running affected versions of Cisco IOS Software and Cisco IOS XE Software are affected when configured to use any of the following features within Cisco IOS:

- Airline Product Set (ALPS)
- Serial Tunnel Code (STUN) and Block Serial Tunnel Code (BSTUN)
- Native Client Interface Architecture support (NCIA)
- Data-link switching (DLSw)
- Remote Source-Route Bridging (RSRB)
- Point to Point Tunneling Protocol (PPTP)
- X.25 for Record Boundary Preservation (RBP)
- X.25 over TCP (XOT)
- X.25 Routing

Information on how to determine whether an affected feature is enabled on a device are provided in the Details section of this advisory.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the "**show version**" command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the "**show version**" command or may provide different output.

The following example identifies a Cisco product that is 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 SOFTWARE (
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 following example shows a product that is 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), Version 12.4
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 about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

<http://www.cisco.com/warp/public/620/1.html> .

☐ **Products Confirmed Not Vulnerable**

The following product and feature have been confirmed not vulnerable:

- Cisco IOS XR Software
- BGP is not affected

No other Cisco products or features configured within Cisco IOS Software are currently known to be affected by this vulnerability.

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

☐ **Details**

Completion of the 3-way handshake to the associated TCP port number(s) of any of the features outlined below is required in order for the vulnerability to be successfully exploited.

Airline Product Set (ALPS)

Devices configured for ALPS are vulnerable. The default TCP listening ports for ALPS are 350 and 10000. The following example shows a vulnerable ALPS configuration:

```
alps local-peer <ip address>
```

Further information about ALPS is available in "Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2 - Configuring the Airline Product Set" at the following link http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcfalps_ps1835_TSD_Products

Serial Tunnel Code (STUN) and Block Serial Tunneling (BSTUN)

Devices configured for either STUN or BSTUN are vulnerable. The default listening TCP ports for STUN are 1990,1991 1992 and 1994. The default listening TCP ports for BSTUN are 1963, 1976, 1977, 1978 and 1979 The following example shows a vulnerable STUN configuration:

```
interface serial 0/0/0  
encapsulation stun
```

The following example shows a vulnerable BSTUN configuration:

```
interface serial 0/0/0  
encapsulation bstun
```

Further information about STUN and BSTUN is available in "Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2 - Configuring Serial Tunnel and Block Serial Tunnel" at the following link http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcfstun_ps1835_TSD_Products

Native Client Interface Architecture support (NCIA)

Devices configured for NCIA are vulnerable, because of the underlying transport they will use. The default listening TCP ports will be dependent on the protocol used with NCIA, such as RSRB or DSLw. The following examples shows a vulnerable configuration:

```
ncia server 1 10.66.91.138 0000.1111.2222 2222.2222.2222 1
```

Further information about NCIA is available in "Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 - Configuring NCIA Client/Server" at the following link http://www.cisco.com/en/US/docs/ios/bridging/configuration/guide/br_ncia_client_svr_ps6350_TSD

Data-link switching (DLSw)

Devices configured for DLSw are vulnerable. The default listening TCP ports for DSLw are 2065, 2067, 1981, 1982 and 1983. The following example shows a vulnerable configuration:

```
dlsw local-peer peer-id <ip address>
```

Devices configured with either FST Encapsulation or Direct Encapsulation are still vulnerable as the affected TCP ports are opened by the "**dslw local-peer peer-id ip address**" command.

Further information about DLSw is available in "Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 - Configuring Data-Link Switching Plus" at the following link http://www.cisco.com/en/US/docs/ios/bridging/configuration/guide/br_dlsw_plus_ps6350_TSD_Prod

Remote Source-Route Bridging (RSRB)

Devices configured for RSRB Using IP Encapsulation over a TCP connection are vulnerable. The default listening TCP ports for RSRB are 1996,1987, 1988 and 1989. The following example shows a vulnerable configuration:

```
source-bridge ring-group 10
source-bridge remote-peer 10 tcp <ip address>
```

Devices configured with either RSRB Using Direct Encapsulation or RSRB Using IP Encapsulation over an FST Connection are not affected.

Further information about RSRB is available in "Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2 - Configuring Remote Source-Route Bridging" at the following link http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcfrsrbr_ps1835_TSD_Products

Point to Point Tunneling Protocol (PPTP)

Devices configured for PPTP are vulnerable. The default listening TCP port for PPTP is 1723. The following examples shows a vulnerable configuration:

```
vpdn enable
!
vpdn-group pptp
! Default PPTP VPDN group
accept-dialin
```

```
protocol pptp
virtual-template 1
```

Or

```
vpdn enable
!
vpdn-group L2_Tunneling
! Default L2TP VPDN group
! Default PPTP VPDN group
accept-dialin
protocol any
virtual-template 1
```

Further information about PPTP is available in "Cisco IOS VPDN Configuration Guide, Release 12.4 - Configuring Client-Initiated Dial-In VPDN Tunneling" at the following link http://www.cisco.com/en/US/docs/ios/vpdn/configuration/guide/client_init_dial-in_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1105140.

X.25 Record Boundary Preservation (RBP)

Devices configured for RBP are vulnerable. The listening TCP port is configured with the "**local port port_number**" CLI command, as shown in the next examples. The following examples shows vulnerable configurations. The first leverages switched virtual circuits (SVC):

```
interface Serial1/0
x25 map rbp 1111 local port <port_number>
```

The second example, leverages a permanent virtual circuit (PVC):

```
interface Serial1/0
x25 map pvc <pvc_number> rbp local port <port_number>
```

Further information about RBP is available in "Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - X.25 Record Boundary Preservation for Data Communications Networks" at the following link http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_x25_rbp_dcn_ps6350_TSD_Pro

X.25 over TCP (XOT)

Devices configured for XOT are vulnerable. The default listening TCP port for XOT is 1998. The following example shows a vulnerable configuration.

```
xot access-group 1

and a corresponding access-list 1.
```

Further information about XOT is available in "Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - X.25 over TCP Profiles" at the following link http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_x25otcp_pro_ps6350_TSD_Pro

X25 Routing

Devices configured with X25 are vulnerable. The default listening TCP port for X25 Routing is 1998. The following example shows a vulnerable configuration.

```
x25 routing
```

Further information about X25 is available in "Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 - Configuring X.25 and LAPB" at the following link http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_cfg_x25_lapb_ps6350_TSD_Pr

This vulnerability is documented in the following Cisco Bug ID: [CSCsr29468](#) ([registered](#) customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0629.

[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>.

CSCsr29468: Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability					
Calculate the environmental score of CSCsr29468					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	

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

☐ Impact

Successful exploitation of this vulnerability will cause the device to reload. Repeated attempts to exploit this vulnerability could result in a sustained 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		
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
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	Vulnerable; first fixed in 12.2SG	12.2(31)SGA9
12.2EWA	Vulnerable; first fixed in 12.2SG	12.2(31)SGA9
12.2EX	Releases prior to 12.2(44)EX are vulnerable, release 12.2(44)EX and later are not vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2EY	12.2(44)EY	12.2(44)SE6
12.2EZ	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2IRA	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4
12.2IRB	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4
12.2IXA	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH
12.2IXB	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH
12.2IXC	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH

12.2IXD	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH
12.2IXE	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH
12.2IXF	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH
12.2IXG	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	
12.2S	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2SB	12.2(33)SB3 12.2(28)SB13 12.2(31)SB14	12.2(33)SB4
12.2SBC	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2SCA	Vulnerable; first fixed in 12.2SCB	12.2(33)SCB1
12.2SCB	12.2(33)SCB1	12.2(33)SCB1
12.2SE	12.2(46)SE2 12.2(50)SE 12.2(44)SE5	12.2(44)SE6
12.2SEA	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEB	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEC	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SED	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEE	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEF	Not Vulnerable	

12.2SEG	Releases prior to 12.2(25) SEG4 are vulnerable, release 12.2(25)SEG4 and later are not vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SG	12.2(50)SG	12.2(52)SG
12.2SGA	12.2(31)SGA9	12.2(31)SGA9
12.2SL	Not Vulnerable	
12.2SM	Vulnerable; contact TAC	
12.2SO	Vulnerable; contact TAC	
12.2SQ	Not Vulnerable	
12.2SRA	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4
12.2SRB	Vulnerable; first fixed in 12.2SRC	12.2(33)SRB5a 12.2(33)SRC4 12.2(33)SRD1
12.2SRC	12.2(33)SRC3	12.2(33)SRC4 12.2(33)SRD1
12.2SRD	12.2(33)SRD1	12.2(33)SRD1
12.2STE	Vulnerable; contact TAC	
12.2SU	Not Vulnerable	
12.2SV	Vulnerable; contact TAC	
12.2SVA	Vulnerable; contact TAC	
12.2SVC	Vulnerable; contact TAC	
12.2SVD	Vulnerable; contact TAC	
12.2SVE	Vulnerable; contact TAC	
12.2SW	Vulnerable; migrate to any release in 12.4SW	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXE	Vulnerable; first fixed in	12.2(18)SXF16

	12.2SXF	
12.2SXF	12.2(18)SXF16	12.2(18)SXF16
12.2SXH	12.2(33)SXH5	12.2(33)SXH5
12.2SXI	12.2(33)SXI1	12.2(33)SXI1
12.2SY	Not Vulnerable	
12.2SZ	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
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	Vulnerable; first fixed in 12.2SRC	12.2(33)SB4 12.2(33)SRD1
12.2XNA	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD1
12.2XNB	12.2(33)XNB1	12.2(33)XNB3
12.2XNC	Not Vulnerable	
12.2XO	12.2(46)XO	12.2(46)XO
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	Vulnerable; first fixed in 12.2SXH	12.2(33)SXH5
12.2ZX	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2ZY	Vulnerable; contact TAC	
12.2ZYA	12.2(18)ZYA1	12.2(18)ZYA1
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
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	12.4(15)MD2 Releases prior to 12.4(11)MD6 are not vulnerable, releases 12.4(15)MD and later are vulnerable.	12.4(11)MD7
12.4MR	12.4(19)MR1 Releases prior to 12.4(16)MR2 are not vulnerable, releases 12.4(19)MR and later are vulnerable	12.4(19)MR2
12.4SW	Not Vulnerable	
	12.4(22)T	

12.4T	12.4(20)T2 Releases prior to 12.4(20) T are NOT vulnerable	12.4(22)T1 12.4(15)T9
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	12.4(15)XQ2	12.4(15)XQ2
12.4XR	12.4(15)XR4	12.4(22)T1 12.4(15)T9
12.4XT	Not Vulnerable	
12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	12.4(15)XY4	12.4(22)T1 12.4(15)T9
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

The following mitigations have been identified for this vulnerability, which may help protect an

infrastructure until an upgrade to a fixed version of Cisco IOS software can be scheduled:

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:

```
!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---
!--- Feature: ALPS
!---

access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 350
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 10000

!---
!--- Deny ALPS TCP traffic from all other sources destined
!--- to infrastructure addresses.
!---

access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 350
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 10000

!---
!--- Feature: STUN
!---

access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1994
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD range 1990 1992

!---
!--- Deny STUN TCP traffic from all other sources destined
!--- to infrastructure addresses.
!---

access-list 150 deny tcp any
```

```
INFRASTRUCTURE_ADDRESSES WILDCARD eq 1994
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD range 1990 1992
```

```
!---
!--- Feature: BSTUN
!---
```

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1963
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD range 1976 1979
```

```
!---
!--- Deny BSTUN TCP traffic from all other sources destined
!--- to infrastructure addresses.
!---
```

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1963
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD range 1976 1979
```

```
!---
!--- Feature: NCIA
!---
```

```
!---
!--- Leverage the underlying protocols, DLSw, RSRB, etc.
!---
```

```
!---
!--- Feature: DLSW
!---
```

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2065
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2067
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD range 1981 1983
```

```
!---
!--- Deny DLSW TCP traffic from all other sources destined
!--- to infrastructure addresses.
!---
```

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2065
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2067
access-list 150 deny tcp any
```

INFRASTRUCTURE_ADDRESSES WILDCARD range 1981 1983

!---

!--- *Feature: RSRB*

!---

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD range 1987 1989
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1996
```

!---

!--- *Deny RSRB TCP traffic from all other sources destined*
!--- *to infrastructure addresses.*

!---

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD range 1987 1989
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1996
```

!---

!--- *Feature: PPTP*

!---

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1723
```

!---

!--- *Deny PPTP TCP traffic from all other sources destined*
!--- *to infrastructure addresses.*

!---

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1723
```

!---

!--- *Feature: RBP*

!---

!--- *RBP will listen for TCP connections on the configured port*
!--- *as per "local port <port_number>". The following example*
!--- *uses port 1055*

!---

```
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1055
```

!---

!--- *Deny RBP traffic from all other sources destined*

```

!--- to infrastructure addresses.
!---

access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1055

!---
!--- Feature: XOT and X.25 Routing
!---

access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1998

!---
!--- Deny XOT and X25 TCP traffic from all other sources
!--- destined to infrastructure addresses.
!---

access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 1998

!---
!--- 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.shtml.

Receive ACLs (rACL)

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 (GSR), 12.0(24)S for the 7500, and 12.0(31)S for the 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor.

Receive ACLs are designed to only protect the device on which it is configured. On the 12000, 7500, and 10720, transit traffic is never affected by a receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below only refer to the router's own physical or virtual IP addresses. Receive ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. 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_paper09186a00801a0a5e.shtml.

The following is the receive path ACL written to permit this type of traffic from trusted hosts:

```
!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---

!---
!--- Permit ALPS traffic from trusted hosts allowed to the RP.
!---

access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 350
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 10000

!---
!--- Deny ALPS traffic from all other sources to the RP.
!---

access-list 150 deny tcp any any eq 350
access-list 150 deny tcp any any eq 10000

!---
!--- Permit STUN traffic from trusted hosts allowed to the RP.
!---

access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 1994
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any range 1990 1992

!---
!--- Deny STUN traffic from all other sources to the RP.
!---

access-list 150 deny tcp any any eq 1994
access-list 150 deny tcp any any eq range 1990 1992
```

```
!---
!--- Permit BSTUN traffic from trusted hosts allowed to the RP.
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 1963
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any range 1976 1979
```

```
!---
!--- Deny BSTUN traffic from all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 1963
access-list 150 deny tcp any any eq range 1976 1979
```

```
!---
!--- Permit DLSw from trusted hosts allowed to the RP.
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 2065
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 2067
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any range 1981 1983
```

```
!---
!--- Deny DLSw all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 2065
access-list 150 deny tcp any any eq 2067
access-list 150 deny tcp any any range 1981 1983
```

```
!---
!--- Permit RSRB traffic from trusted hosts allowed to the RP.
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 1996
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any range 1987 1989
```

```
!---
!--- Deny RSRB traffic from all other sources to the RP.
!---
```

```
access-list 150 deny tcp any any eq 1996
```

```
access-list 150 deny tcp any any range 1987 1989
```

```
!---  
!--- Permit PPTP traffic from trusted hosts allowed to the RP.  
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 1723
```

```
!---  
!--- Deny PPTP traffic from all other sources to the RP.  
!---
```

```
access-list 150 deny tcp any any eq 1723
```

```
!---  
!--- Permit RBP traffic from trusted hosts allowed to the RP.  
!--- RBP will listen for TCP connections on the configured port  
!--- as per "local port <port_number>". The following example  
!--- uses port 1055  
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 1055
```

```
!---  
!--- Deny RBP traffic from all other sources to the RP.  
!---
```

```
access-list 150 deny tcp any any eq 1055
```

```
!---  
!--- Permit XOT and X.25 Routing traffic from trusted hosts allowed  
!--- to the RP.  
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 1998
```

```
!---  
!--- Deny XOT and X.25 Routing traffic from all other sources to  
!--- the RP.  
!---
```

```
access-list 150 deny tcp any any eq 1998
```

```
!--- Permit all other traffic to the RP.
```

```
!--- according to security policy and configurations.
```

```
access-list 150 permit ip any any
```

```
!--- Apply this access list to the 'receive' path.
```

```
ip receive access-list 150
```

Control Plane Policing

Control Plane Policing (CoPP) can be used to block the affected features TCP traffic 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 that will protect all devices with IP addresses in the infrastructure IP address range.

```
!---  
!--- Only sections pertaining to features enabled on the device  
!--- need be configured.
```

```
!---  
!--- Feature: ALPS  
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD any eq 350  
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD any eq 10000
```

```
!---  
!--- Permit ALPS 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 150 permit tcp any any eq 350  
access-list 150 permit tcp any any eq 10000
```

```
!---  
!--- Feature: STUN  
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD  
any eq 1994  
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD  
any range 1990 1992
```

```
!---  
!--- Permit STUN 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 150 permit tcp any any eq 1994
access-list 150 permit tcp any any range 1990 1992
```

```
!---
!--- Feature: BSTUN
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any eq 1963
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any range 1976 1979
```

```
!---
!--- Permit BSTUN 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 150 permit tcp any any eq 1963
access-list 150 permit tcp any any range 1976 1979
```

```
!---
!--- Feature: NCIA
!---
!--- Leverage the underlying protocols, DLSw, RSRB, etc.
!---
```

```
!---
!--- Feature: DLSW
!---
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any eq 2065
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any eq 2067
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any range 1981 1983
```

```
!---
!--- Permit DLSW 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 150 permit tcp any any eq 2065
access-list 150 permit tcp any any eq 2067
access-list 150 permit tcp any any range 1981 1983
```

!---

!--- *Feature: RSRB*

!---

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any range 1987 1989
```

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any eq 1996
```

!---

!--- *Permit RSRB 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 150 permit tcp any any range 1987 1989
```

```
access-list 150 permit tcp any any eq 1996
```

!---

!--- *Feature: PPTP*

!---

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any eq 1723
```

!---

!--- *Permit PPTP 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 150 permit tcp any any eq 1723
```

!---

!--- *Feature: RBP*

!---

!--- *RBP will listen for TCP connections on the configured port*

!--- *as per "local port <port_number>". The following example*

!--- *uses port 1055*

```
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
    any eq 1055
```

!---

!--- *Permit RBP 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 150 permit tcp any any eq 1055

!---
!--- Feature: XOT and X.25 Routing
!---

access-list 150 deny tcp TRUSTED_HOSTS WILDCARD
      any eq 1998

!---
!--- Permit XOT and X25 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 150 permit tcp any any eq 1998

!---
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- configurations for traffic that is authorized to be sent
!--- and to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
!---

class-map match-all drop-tcp-class
  match access-group 150

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

policy-map drop-tcp-traffic
  class drop-tcp-class
    drop

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

control-plane
  service-policy input drop-tcp-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-tcp-traffic
class drop-tcp-class
police 32000 1500 1500 conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, "Control Plane Policing Implementation Best Practices" and "Cisco IOS Software Releases 12.2 S - Control Plane Policing" at the following links

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.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, at the following link <http://www.cisco.com/warp/public/707/cisco-amb-20090325-tcp-and-ip.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, 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

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 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 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-20090325-tcp.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-bulletins@lists.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	2009- July-06	Removed references to software availability dates.
Revision 1.1	2009- June-26	Removed references to the March/09 combined fixed software table.
Revision 1.0	2009- March-25	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. 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)

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.](#)