

TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products

Advisory ID: [cisco-sa-20090908-tcp24](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>

Revision 1.3

Last Updated 2009 September 28 1400 UTC (GMT)

For Public Release 2009 September 8 1700 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

Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

The following Cisco products have a TCP implementation that is affected by these vulnerabilities. Refer to the Software Versions and Fixes section for information on fixed software.

Cisco IOS Software

To determine the Cisco IOS[®] Software release that is running on a Cisco product, administrators can log into 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 (fc2)
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 identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
RELEASE SOFTWARE (fc3)
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/web/about/security/intelligence/ios-ref.html>

Cisco IOS-XE Software

The version of Cisco IOS-XE Software that is running on a Cisco product can be determined using the **show version** command from the Command Line Interface (CLI).

Cisco CatOS Software

The version of Cisco CatOS Software that is running on a Cisco product can be determined using the **show version** command from the CLI.

Cisco Adaptive Security Appliance (ASA) and Cisco PIX

Cisco ASA and Cisco PIX security appliances running versions 7.1, 7.2, 8.0, and 8.1 are affected when configured for any of the following features:

- SSL VPNs
- ASDM Administrative Access
- Telnet Access
- SSH Access
- Cisco Tunneling Control Protocol (cTCP) for Remote Access VPNs
- Virtual Telnet
- Virtual HTTP
- Transport Layer Security (TLS) Proxy for Encrypted Voice Inspection
- Cut-Through Proxy for Network Access

The version of software that is running on a Cisco ASA and Cisco PIX security appliances can be determined using the **show version** command from the CLI.

Cisco NX-OS Software

The version of Cisco NX-OS Software that is running on Cisco Nexus 5000 and 7000 series devices can be determined using the **show version** command from the CLI.

Scientific Atlanta Products

Scientific Atlanta customers are instructed to contact Scientific Atlanta's Technical Support for questions regarding the impact, mitigation and remediation of the vulnerabilities discussed in this document.

Contact information for Scientific Atlanta Technical Support can be found at the following web site:

http://www.cisco.com/en/US/products/ps10459/serv_group_home.html

Linksys Products

Cisco has investigated the Linksys product family and found that no Linksys products are affected by the TCP vulnerabilities. Customers with additional questions on Linksys products should contact:

security@linksys.com

☐ Products Confirmed Not Vulnerable

The following Cisco products are not affected:

- Cisco IOS XR
- Cisco IOS Software Modularity
- Cisco ASA Software version 8.2
- Cisco ASA and Cisco PIX Software version 7.0

- Cisco PIX Software version 6.x and earlier
- Cisco Firewall Services Module (FWSM)
- Cisco Multilayer Distribution Switches (MDS)
- Cisco Application Control Engine (ACE) Modules and Appliances
- Cisco ACE XML Gateway
- Cisco Access Control Server (ACS) Solution Engine
- Cisco Guard
- Cisco Security Monitoring, Analysis, and Response System (CS-MARS)
- Cisco ONS 15000
- Cisco Content Services Switches (CSS)
- Cisco Wide Area Application Services (WAAS)
- Cisco Wireless LAN Controller (WLC)
- IronPort C, M, S and X Series Appliances
- Cisco Global Site Selector (GSS)
- Cisco SSL Services Module (SSLM)
- Cisco Network Analysis Module (NAM)
- Cisco Content Switch Module (CSM)
- Cisco Web Application Firewall (WAF)
- Cisco Service Control Engine (SCE)
- Cisco Wireless Services Modules (WiSM)
- Cisco Application and Content Networking System (ACNS)
- Cisco Content Engine (CE)

Cisco PSIRT tested Cisco products that are based on Linux and Microsoft Windows operating systems and found that although TCP connections in a FINWAIT1 state may temporarily consume system resources the operating systems eventually clear the TCP connections. If enough system resources are consumed, a sustained DoS condition may be possible. This outcome is highly dependent on the configuration and usage of a system. For more information about how these vulnerabilities affect Microsoft Windows operating systems, please consult the following Microsoft website at the following link:

<http://go.microsoft.com/fwlink/?LinkId=155978> 

No other Cisco products are currently known to be affected by these vulnerabilities.

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

☐ Details

Multiple Cisco products are affected by DoS vulnerabilities in the TCP protocol. By manipulating the state of TCP connections, an attacker could force a system that is under attack to maintain TCP connections for long periods of time, or indefinitely in some cases. With a sufficient number of open TCP connections, the attacker may be able to cause a system to consume internal buffer and memory resources, resulting in new TCP connections being denied access to a targeted port or an entire system. A system reboot may be required to restore full system functionality. A full TCP three-way handshake is required to exploit these vulnerabilities.

Network devices are not directly impacted by TCP state manipulation DoS attacks transiting a device; however, network devices that maintain the state of TCP connections may be impacted. If the attacker can establish enough TCP connections through a transit device that maintains TCP state, device resources may be exhausted and prevent the device from processing new TCP connections, resulting in a DoS condition. If an affected device that forwards traffic (that is, routes) in a network is the target of a TCP state manipulation attack, the attacker could cause a network-impacting DoS condition.

Cisco IOS Software

All Cisco IOS Software versions are affected by this vulnerability. A device running Cisco IOS Software that is under attack will have numerous hung TCP connections in the FINWAIT1 state. The **show tcp brief** command can be used to display the hung TCP connections. The following is example output showing an attack in progress.

```
Router#show tcp brief | include FIN
63D697C4 192.168.1.10.80          192.168.1.20.38479          FINWAIT1
63032A28 192.168.1.10.80          192.168.1.20.54154          FINWAIT1
645F8068 192.168.1.10.80          192.168.1.20.56287          FINWAIT1
630323F4 192.168.1.10.80          192.168.1.20.6372           FINWAIT1
63D69190 192.168.1.10.80          192.168.1.20.23489          FINWAIT1
```

The vulnerabilities for Cisco IOS Software are documented in Cisco Bug ID [CSCsv04836](#) ([registered](#) customers only) .

Cisco IOS-XE Software

All Cisco IOS-XE Software versions are affected by this vulnerability. A device running Cisco IOS-XE Software that is under attack will have numerous hung TCP connections in the FINWAIT1 state. The **show tcp brief** command can be used to display the hung TCP connections. The following is example output showing an attack in progress.

```
Router#show tcp brief | include FIN
63D697C4 192.168.1.10.80          192.168.1.20.38479          FINWAIT1
63032A28 192.168.1.10.80          192.168.1.20.54154          FINWAIT1
645F8068 192.168.1.10.80          192.168.1.20.56287          FINWAIT1
630323F4 192.168.1.10.80          192.168.1.20.6372           FINWAIT1
63D69190 192.168.1.10.80          192.168.1.20.23489          FINWAIT1
```

The vulnerabilities for Cisco IOS-XE Software are documented in Cisco Bug ID [CSCsv07712](#) ([registered](#) customers only) .

Cisco CatOS Software

All Cisco CatOS Software versions are affected by these vulnerabilities. A device running Cisco CatOS Software that is under attack will have numerous hung TCP connections in the FIN_WAIT_1 state. The **show netstat** command can be used to display the hung TCP connections. The following is example output showing an attack in progress.

```
Console> (enable) show netstat
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp 0 83 192.168.1.10.23 192.168.1.20.46056 FIN_WAIT_1
tcp 0 83 192.168.1.10.23 192.168.1.20.16305 FIN_WAIT_1
tcp 0 83 192.168.1.10.23 192.168.1.20.14628 FIN_WAIT_1
tcp 0 83 192.168.1.10.23 192.168.1.20.7275 FIN_WAIT_1
tcp 0 83 192.168.1.10.23 192.168.1.20.39559 FIN_WAIT_1
```

The vulnerabilities for Cisco CatOS Software are documented in Cisco Bug ID [CSCsv66169](#) ([registered](#) customers only) .

Cisco ASA and Cisco PIX Software

Certain Cisco ASA and Cisco PIX Software versions are affected by these vulnerabilities. A device running Cisco ASA and Cisco PIX Software that is under attack will have numerous TCP connections in the established state. The **show asp table socket** command can be used to display the TCP connections. The following is example output showing a potential attack in progress.

```
FIREWALL# show asp table socket | grep ESTAB
TCP 123a8a6c 192.168.1.10:80 192.168.1.20:46181 ESTAB
TCP 123e6d54 192.168.1.10:80 192.168.1.20:29546 ESTAB
TCP 1244f78c 192.168.1.10:80 192.168.1.20:40271 ESTAB
TCP 124f8d2c 192.168.1.10:80 192.168.1.20:46599 ESTAB
```

```
TCP          12507f2c  192.168.1.10:80          192.168.1.20:5607      ESTAB
```

It is possible for normal traffic to cause established TCP connections to appear on Cisco ASA or PIX devices, especially VPN connections terminated to the device. In order to confirm if established TCP connections are part of an attack, administrators should use a monitoring point outside the firewall such as a packet sniffer or Netflow collection agent to examine the profile of the suspicious TCP connections and determine if an attack is occurring.

Note: The **show asp table socket** command was introduced in Cisco ASA and Cisco PIX Software 8.0(1).

Further detail about hung TCP connections can be found with **show conn detail all long** command. The IP address used to qualify the example below is the address of the firewall interface under attack.

```
FIREWALL# show conn detail all long | grep 192.168.1.10
TCP outside:192.168.1.20/62345 (192.168.1.20/62345) NP Identity Ifc:192.168.1.10/80
(192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
TCP outside:192.168.1.20/56268 (192.168.1.20/56268) NP Identity Ifc:192.168.1.10/80
(192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
TCP outside:192.168.1.20/63445 (192.168.1.20/63445) NP Identity Ifc:192.168.1.10/80
(192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
TCP outside:192.168.1.20/49151 (192.168.1.20/49151) NP Identity Ifc:192.168.1.10/80
(192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
TCP outside:192.168.1.20/57147 (192.168.1.20/57147) NP Identity Ifc:192.168.1.10/80
(192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
```

Note: Both troubleshooting commands referenced about will display TCP connections that are terminated to a firewall interface and transiting through the firewall.

The vulnerabilities for Cisco ASA and Cisco PIX Software are documented in Cisco Bug ID [CSCsv02768](#) ([registered](#) customers only) .

Cisco NX-OS Software

All Cisco Nexus 5000 and 7000 platforms running Cisco NX-OS Software are affected by these vulnerabilities. A Nexus 5005 or 7000 device running Cisco NX-OS Software that is under attack will have numerous hung TCP connections in the FIN_WAIT_1 state. The **show tcp connection detail** command can be used to display the hung TCP connections. The following is example output showing an attack in progress.

```
NEXUS# show tcp connection detail | include FIN
State: FIN_WAIT_1
State: FIN_WAIT_1
State: FIN_WAIT_1
State: FIN_WAIT_1
State: FIN_WAIT_1
```

The hung TCP connection vulnerabilities for Nexus 5000 and Nexus 7000 devices are documented in Cisco Bug ID [CSCsv08325](#) ([registered](#) customers only) and Cisco Bug ID [CSCsv08579](#) ([registered](#) customers only) respectively.

While investigating the TCP state manipulation vulnerabilities, it was discovered that Cisco NX-OS on Nexus 5000 platforms may be vulnerable to a system crash when receiving a specific sequence of TCP packets. This vulnerability is documented in Cisco Bug ID [CSCsv08059](#) ([registered](#) customers only) and has been assigned CVE identifier CVE-2009-0627.

The TCP state manipulation vulnerabilities have been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-4609.

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

☐ Vulnerability Scoring Details

Cisco has provided 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.

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>

CSCsv04836 - Connections getting stuck at FINWAIT1 state (registered customers only)					
Calculate the environmental score of CSCsv04836					
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	
Functional		Official-Fix		Confirmed	

CSCsv07712 - Connections getting stuck at FINWAIT1 state (registered customers only)					
Calculate the environmental score of CSCsv07712					
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	
Functional		Official-Fix		Confirmed	

<u>CSCsv66169 - TCP Connections get stuck in FINWAIT1 state (registered customers only)</u>					
Calculate the environmental score of <u>CSCsv66169</u>					
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	
Functional		Official-Fix		Confirmed	

<u>CSCsv02768 - TCP connections getting stuck in FINWAIT1 state (registered customers only)</u>					
Calculate the environmental score of <u>CSCsv02768</u>					

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
Functional	Official-Fix	Confirmed

[CSCsv08325 - TCP connections may get stuck in any state after ESTAB indefinitely \(registered customers only\)](#)

Calculate the environmental score of [CSCsv08325](#)

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
Functional	Official-Fix	Confirmed

[CSCsv08579 - TCP connections get stuck in FINWAIT1 state indefinitely \(registered customers only\)](#)

Calculate the environmental score of [CSCsv08579](#)

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
Functional	Official-Fix	Confirmed

[CSCsv08059 - NEXUS 5000 crashes after certain TCP packets \(registered customers only\)](#)

Calculate the environmental score of [CSCsv08059](#)

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
Functional	Official-Fix	Confirmed

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

☐ Impact

Successful exploitation of the TCP state manipulation vulnerabilities may result in a DoS condition where new TCP connections are not accepted on an affected system. Repeated exploitation may result in a sustained DoS condition. A reboot may be required to recover affected systems.

In addition, Cisco Nexus 5000 systems may crash upon receiving a specific sequence of TCP packets.

[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.

Cisco IOS Software

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	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0DA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
		12.4(15)T10

12.0DB	Vulnerable; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.0DC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0S	12.0(33)S3 12.0(32)S12	12.0(33)S5 12.0(32)S14; Available on 25-SEP-2009
12.0SC	Vulnerable; first fixed in 12.0S	12.0(33)S5 12.0(32)S14; Available on 25-SEP-2009
12.0SL	Vulnerable; first fixed in 12.0S	12.0(33)S5 12.0(32)S14; Available on 25-SEP-2009
12.0SP	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0ST	Vulnerable; first fixed in 12.0S	12.0(33)S5 12.0(32)S14; Available on 25-SEP-2009
12.0SX	Vulnerable; first fixed in 12.0S	12.0(33)S5 12.0(32)S14; Available on 25-SEP-2009

12.0SY	12.0(32)SY8 12.0(32)SY9a 12.0(32)SY10 ; Available on 25-SEP-2009	12.0(32)SY9a 12.0(32)SY10; Available on 25-SEP-2009
12.0SZ	12.0(30)SZ10	12.0(33)S5 12.0(32)S14; Available on 25-SEP-2009
12.0T	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0W	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.0WC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.0WT	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XB	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.0XC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XE	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XF	Vulnerable; first fixed in 12.4	
12.0XG	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XH	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XI	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XJ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XK	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XL	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XM	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.0XN	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XQ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XR	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.0XS	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.0XT	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XV	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
Affected 12.1- Based Releases	First Fixed Release	Recommended Release
12.1	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.1AA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1AX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1AY	Vulnerable; first fixed in 12.1EA	12.1(22)EA13
12.1AZ	Vulnerable; first fixed in 12.1EA	12.1(22)EA13
12.1CX	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1DA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1DB	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1DC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1E	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1EA	12.1(22)EA13	12.1(22)EA13

12.1EB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1EC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1EO	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1EU	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1EV	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1EW	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1EX	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1EY	12.2(44)EY	12.2(46)EY
12.1EZ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1GA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.1GB	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1T	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XB	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XE	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XF	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XG	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XH	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
		12.4(23b)

12.1XI	Vulnerable; first fixed in 12.4	12.4(25b)
12.1XJ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XL	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XM	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XP	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XQ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XR	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XS	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.1XT	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XU	Vulnerable; first fixed in 12.4	12.4(23b)

		12.4(25b)
12.1XV	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XW	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XX	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XY	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XZ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YB	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YE		12.4(15)T10 12.4(20)T4

	Vulnerable; first fixed in 12.4T	12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.1YF	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YH	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YI	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1YJ	Vulnerable; first fixed in 12.1EA	12.1(22)EA13
Affected 12.2- Based Releases	First Fixed Release	Recommended Release
12.2	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2B	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2BC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2BW	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.2BX	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2BY	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2BZ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2CX	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2CY	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2CZ	Vulnerable; first fixed in 12.2SB	12.2(28)SB14; Available on 20-OCT-2009
12.2DA	12.2(12)DA14	12.4(25b) 12.4(23b)
12.2DD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2DX	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2EW	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2EWA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2EX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2EY	Releases prior to 12.2(44)EY are vulnerable, release 12.2(44)EY and later are not vulnerable	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2EZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2FX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2FY	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2FZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IRA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IRB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of	

	this advisory	
12.2IRC	12.2(33)IRC	
12.2IXA	Vulnerable; migrate to any release in 12.2IXH	
12.2IXB	Vulnerable; migrate to any release in 12.2IXH	
12.2IXC	Vulnerable; migrate to any release in 12.2IXH	
12.2IXD	Vulnerable; migrate to any release in 12.2IXH	
12.2IXE	Vulnerable; migrate to any release in 12.2IXH	
12.2IXF	Vulnerable; migrate to any release in 12.2IXH	
12.2IXG	Vulnerable; migrate to any release in 12.2IXH	
12.2IXH	12.2(18)IXH	
12.2JA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2JK	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.2MB	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2MC	12.2(15)MC2m	12.4(25b) 12.4(23b)
12.2S	Vulnerable; first fixed in 12.2SB	12.2(28)SB14; Available on 20-OCT-2009
12.2SB	12.2(28)SB13 12.2(31)SB14 12.2(33)SB1b 12.2(34)SB2	12.2(31)SB16 12.2(28)SB14; Available on 20-OCT-2009 12.2(33)SB7
12.2SBC	Vulnerable; first fixed in 12.2SB	12.2(28)SB14; Available on 20-OCT-2009
12.2SCA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SCB	12.2(33)SCB1	12.2(33)SCB4
12.2SE	12.2(44)SE5 12.2(46)SE2 12.2(50)SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SEA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2SEB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SEC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SED	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SEE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SEF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SEG	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SG	12.2(50)SG	12.2(53)SG1
12.2SGA	12.2(31)SGA9	12.2(31)SGA11; Available on 04-DEC-2009
12.2SL	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2SM	Releases prior to 12.2(29)SM5 are	

	vulnerable, release 12.2(29)SM5 and later are not vulnerable	12.2(29)SM5
12.2SO	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SQ	12.2(44)SQ2	
12.2SRA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SRB	12.2(33)SRB5a	12.2(33)SRD3 12.2(33)SRC5; Available on 29-OCT-2009
12.2SRC	12.2(33)SRC3	12.2(33)SRC5; Available on 29-OCT-2009
12.2SRD	12.2(33)SRD1	12.2(33)SRD3
12.2STE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SU	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2SV	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2SVA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SVC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SVD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SVE	12.2(29)SVE1	
12.2SW	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.2SX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	12.2(18)SXF17; Available on 30-SEP-2009

12.2SXD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXF	12.2(18)SXF16	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXH	12.2(33)SXH5	12.2(33)SXH6; Available on 30-OCT-2009
12.2SXI	12.2(33)SXI1	12.2SXI2a
12.2SY	Vulnerable; first fixed in 12.2SB	12.2(28)SB14; Available on 20-OCT-2009
12.2SZ	Vulnerable; first fixed in 12.2SB	12.2(28)SB14; Available on 20-OCT-2009
12.2T	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2TPC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2XA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.2XB	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XE	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XF	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XG	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XH	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XI	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XJ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XK	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XL		12.4(23b)

	Vulnerable; first fixed in 12.4	12.4(25b)
12.2XM	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XN	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2XNA	Please see Cisco IOS-XE Software Availability	
12.2XNB	Please see Cisco IOS-XE Software Availability	
12.2XNC	Please see Cisco IOS-XE Software Availability	
12.2XND	Please see Cisco IOS-XE Software Availability	
12.2XO	12.2(52)XO	12.2(50)SG5; Available on 28-SEP-2009
12.2XQ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XR	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XS	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.2XT	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XU	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XV	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XW	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2YA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2YB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

	btaining Fixed Software section of this advisory	
12.2YG	Vulnerable; Contact your support organization per the instructions in Q btaining Fixed Software section of this advisory	
12.2YH	Vulnerable; Contact your support organization per the instructions in Q btaining Fixed Software section of this advisory	
12.2YJ	Vulnerable; Contact your support organization per the instructions in Q btaining Fixed Software section of this advisory	
12.2YK	Vulnerable; Contact your support organization per the instructions in Q btaining Fixed Software section of this advisory	
12.2YL	Vulnerable; Contact your support organization per the instructions in Q btaining Fixed Software section of this advisory	
12.2YM	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2YN	Vulnerable; Contact your support organization per the instructions in Q btaining Fixed Software section of this advisory	
12.2YO	Vulnerable; Contact your support organization per the instructions in Q btaining Fixed Software section of this advisory	

12.2YP	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.2YQ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YR	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YS	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YT	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YU	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YV	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YW	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2YX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YY	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	12.2(18)SXF17; Available on 30-SEP-2009
12.2ZB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZE	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZF	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.2ZG	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZH	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZJ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZM	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZP	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZU	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZX	Vulnerable; first fixed in 12.2SB	12.2(28)SB14; Available on 20-OCT-2009
12.2ZY	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2ZYA	12.2(18)ZYA1	12.2(18)ZYA2
Affected 12.3- Based Releases	First Fixed Release	Recommended Release
12.3	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3B	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3BC	12.3(21a)BC9 12.3(23)BC6	12.3(21a)BC9
12.3BW	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3EU	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3JA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3JEA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3JEB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.3JEC	12.3(8)JEC3	
12.3JED	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3JK	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3JL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3JX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3T	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3TPC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3VA	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
		12.4(23b)

12.3XA	Vulnerable; first fixed in 12.4	12.4(25b)
12.3XB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3XC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XE	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3XG	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XI	Vulnerable; first fixed in 12.2SB	12.2(33)SB7 12.2(31)SB16
12.3XJ	Vulnerable; first fixed in 12.4XR	12.4(15)XR7 12.4(22)XR
12.3XK	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.3XL	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XQ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XR	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XS	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XU	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3XW	Vulnerable; first fixed in 12.4XR	12.4(15)XR7 12.4(22)XR
12.3XX	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XY	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XZ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3YA		12.4(23b)

	Vulnerable; first fixed in 12.4	12.4(25b)
12.3YD	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YF	Vulnerable; first fixed in 12.4XR	12.4(15)XR7 12.4(22)XR
12.3YG	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YH	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YI	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.3YJ	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YK	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YM	12.3(14)YM13	12.4(23b) 12.4(25b)
12.3YQ	Vulnerable; first fixed in 12.4T	12.4(23b) 12.4(25b)
12.3YS	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YT	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.3YU	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YX	12.3(14)YX14	12.4(15)XR7 12.4(22)XR
12.3YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3ZA	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
Affected 12.4-Based Releases	First Fixed Release	Recommended Release
12.4	12.4(18d) 12.4(23a) 12.4(25)	12.4(25b) 12.4(23b)
12.4GC	12.4(22)GC1 12.4(24)GC1	12.4(24)GC1
12.4JA	12.4(16b)JA1	

	12.4(21a)JA	
12.4JDA	12.4(10b)JDA3	
12.4JDC	12.4(10b)JDC	
12.4JDD	12.4(10b)JDD	
12.4JK	12.4(3)JK4	
12.4JL	12.4(3)JL1	
12.4JMA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4JMB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4JX	12.4(21a)JX	
12.4MD	12.4(11)MD7 12.4(15)MD2 12.4(22)MD	12.4(11)MD9 12.4(15)MD3 12.4(22)MD1
12.4MDA	12.4(22)MDA	12.4(22)MDA1
12.4MR		

	12.4(19)MR2	12.4(19)MR3
12.4SW	12.4(15)SW3	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4T	12.4(5)T5e 12.4(15)T6a 12.4(22)T1 12.4(20)T2 12.4(24)T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XA	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XB	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XC	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3

		12.4(24)T2; Available on 23-OCT-2009
12.4XD	12.4(4)XD12	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XE	12.4(6)XE4	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XF	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XG	12.4(9)XG4	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XJ	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3

		12.4(24)T2; Available on 23-OCT-2009
12.4XK	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XL	12.4(15)XL4	
12.4XM	12.4(15)XM3	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XN	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4XP	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4XQ	12.4(15)XQ2	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.4XR	12.4(15)XR4 12.4(22)XR	12.4(15)XR7
12.4XT	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XV	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4XW	12.4(11)XW10	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XY	12.4(15)XY4	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XZ	12.4(15)XZ2	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.4YA	12.4(20)YA2	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YB	12.4(22)YB	12.4(22)YB4
12.4YD	12.4(22)YD	12.4(22)YD1
12.4YE	12.4(22)YE	12.4(22)YE1

Cisco IOS-XE Software

IOS-XE Release	First Fixed Release
2.1.x	2.2.3
2.2.x	2.2.3
2.3.x	Not Vulnerable
2.4.x	Not Vulnerable

Cisco CatOS Software

Affected Releases	First Fixed Release
7.x	7.6(24a)

8.x	8.7(2a)
-----	---------

Cisco ASA and Cisco PIX Software

Affected Releases	First Fixed Release
7.1	7.1(2.79)
7.2	7.2(4.18)
8.0	8.0(4.9)
8.1	8.1(2.3)
8.2	Not Vulnerable

Cisco NX-OS Software

Affected Releases	First Fixed Release
Cisco Nexus 5000	4.0(1a)N2(1)
Cisco Nexus 7000	4.1(4)

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

Workarounds

It is possible to mitigate these vulnerabilities with the following workarounds.

Cisco IOS Software

The Cisco Guide to Harden Cisco IOS Devices provides examples of many useful techniques to mitigate against the TCP state manipulation vulnerabilities. These include:

- Infrastructure Access Control Lists (iACL)
- Receive Access Control Lists (rACL)

- Transit Access Control Lists (tACL)
- VTY Access Control Lists
- Control Plane Policing (CoPP)
- Control Plane Protection (CPPr)
- Management Plane Policing (MPP)

For more information on the topics listed above, consult the Cisco Guide to Harden Cisco IOS Devices at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Cisco CatOS Software

Cisco CatOS software provides VLAN Access Control Lists (VACL) to mitigate against the TCP state manipulation vulnerabilities. For more information on configuring VACLs on CatOS 7.x software versions, please consult the following link:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/7.x/configuration/guide/acc_list.html

For more information on configuring VACLs on CatOS 8.x software versions, please consult the following link:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/acc_list.html

Cisco ASA and Cisco PIX Software

Cisco ASA and Cisco PIX Software provide a method to expire stalled half-closed TCP connections that helps mitigate against the TCP state manipulation vulnerabilities. This method protects against attacks directed to a firewall and devices protected by a firewall. The **timeout half-closed** command will expire TCP sessions that have remained in a half-closed state beyond a user-configured timeout.

```
FIREWALL(config)# timeout half-closed 0:5:0
```

This command will set the TCP half-closed timeout to the smallest permitted value of five minutes. For more information on the TCP half-closed timeout, please consult the following link:

<http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/t.html#wp1500148>

Cisco Nexus Software

Cisco Nexus software provides several ACL methods to mitigate against the TCP state manipulation vulnerabilities. For more information on configuring ACLs on Nexus 5000 systems, please consult the following link:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/sec_ipacis.html

For more information on configuring ACLs on Nexus 7000 systems, please consult the following link:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg.html

Cisco Applied Mitigation Bulletin

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:

<http://www.cisco.com/warp/public/707/cisco-amb-20090908-tcp24.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.

The TCP state manipulation vulnerability was coordinated by CERT-FI based on research referenced in their public advisory. To view their advisory and credited references, please refer to:

<https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html> 

The TCP proof-of-concept tool, known as Sockstress, was provided to Cisco by Robert E. Lee and Jack Louis of Outpost24. The Cisco Nexus vulnerability was discovered by Cisco.

[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-20090908-tcp24.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 1.3	2009-September-28	Added to Products Confirmed Not Vulnerable list; updated software table.
Revision 1.2	2009-September-16	Revised the Affected Products section for Linksys products and the Exploitation and Public Announcements section
Revision 1.1	2009-September-11	Updated vulnerable software
Revision 1.0	2009-September-08	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](#)

© 2010 - 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)