

Cisco Security Advisory: Cisco IOS Software Tunnels Vulnerability

Advisory ID: cisco-sa-20090923-tunnels

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>

Revision 1.3

Last Updated 2009 October 19 1600 UTC (GMT)

For Public Release 2009 September 23 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 devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

Note: The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

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

☐ Affected Products

Cisco devices are vulnerable when running an affected version of Cisco IOS Software and configured for Generic Routing Encapsulation (GRE), IPinIP, Generic Packet Tunneling in IPv6 or IPv6 over IP tunnels with Cisco Express Forwarding enabled. The Cisco IOS Point to Point Tunneling Protocol (PPTP) feature creates GRE tunnels that are transparent to the user. Therefore systems configured for PPTP are also vulnerable.

The Cisco multicast Virtual Private Network (MVPN) feature also creates GRE tunnels that are transparent to the user, however MVPN configurations are not vulnerable, unless there are other tunnels that are configured explicitly.

☐ Vulnerable Products

A Cisco IOS device that is explicitly configured for a tunnel will have a configuration similar to the following in the output of **show running-config**:

```
interface tunnel0
  ip address [IP-address]
  tunnel source [Tunnel-Source]
  tunnel destination [Tunnel Destination]
```

An alternative method to identify devices that are configured for tunnels is to use the **show interfaces** command. A sample output is provided below:

```
Router#show interfaces | include Tunnel
Tunnel0 is up, line protocol is down
  Hardware is Tunnel
  [...]
  Tunnel protocol/transport GRE/IP
```

!-- output truncated

A Cisco IOS device that is configured for Cisco Express Forwarding will display the forwarding table in the output of **show ip cef** output, as in the following example:

```
Router#show ip cef
Prefix                Next Hop                Interface
0.0.0.0/0             10.48.64.1             Ethernet0/0
0.0.0.0/32            receive
.....
```

Cisco Express Forwarding is enabled by default in most Cisco IOS Software versions.

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 7200 series device running Cisco IOS Software release 12.3(19) with an installed image name of C7200-JS-M:

```
7200#show version
Cisco Internetwork Operating System Software
```

```
IOS (tm) 7200 Software (C7200-JS-M), Version 12.3(19),  
RELEASE SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2006 by cisco Systems, Inc.  
Compiled Thu 11-May-06 22:37 by evmiller
```

!-- output truncated

The following example identifies a Cisco 7300 series device running Cisco IOS Software release 12.3(22) with an installed image name of C7301-P-M:

```
7301# show version  
Cisco Internetwork Operating System Software  
IOS (tm) 7301 Software (C7301-P-M), Version 12.3(22),  
RELEASE SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2007 by cisco Systems, Inc.  
Compiled Wed 24-Jan-07 20:26 by ccai
```

!-- 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**

Cisco IOS XR Software is not affected.

Cisco IOS XE Software is not affected.

IPsec and Dynamic Multipoint VPN (DMVPN) configurations that are protected by IPsec are not affected.

MVPN configurations are not affected.

Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) tunnels are not affected.

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

☐ Details

A tunnel protocol encapsulates a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between internetworking devices over an IP network.

Cisco Express Forwarding is a Layer 3 IP switching technology. It improves network performance and scalability for networks with high and dynamic traffic patterns.

Devices that are running Cisco IOS Software and configured for GRE, IPinIP, Generic Packet Tunneling in IPv6 or IPv6 over IP tunnels and Cisco Express Forwarding may reload upon switching a specially crafted malformed packets. Please note that using PPTP creates GRE tunnels that are transparent to the end user so devices configured for PPTP are vulnerable if they are configured on an affected software version. Using MVPN also creates GRE tunnels that are transparent to the end user. However MVPN configurations are not vulnerable.

These vulnerabilities are addressed by the Cisco Bug IDs [CSCsh97579](#) ([registered](#) customers only) , [CSCsq31776](#) ([registered](#) customers only) and [CSCsx70889](#) ([registered](#) customers only) and have been assigned Common Vulnerabilities and Exposures (CVE) IDs CVE-2009-2872 and CVE-2009-2873.

☐ 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>.

CSCsh97579 - switching bad packet tunnel to tunnel crashes router

Calculate the environmental score of [CSCsh97579](#)

CVSS Base Score - **7.1**

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

CVSS Temporal Score - **5.9**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsq31776 - ip tunnels regression test can crash the router

Calculate the environmental score of [CSCsq31776](#)

CVSS Base Score - **7.1**

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

CVSS Temporal Score - **5.9**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsx70889 - Systems configured for tunnels reload after receiving malformed packets

Calculate the environmental score of [CSCsx70889](#)

CVSS Base Score - **7.1**

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

CVSS Temporal Score - **5.9**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

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

[-] Impact

Successful exploitation of the vulnerability may result in the reload of an affected system, causing a 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
12.0	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0DA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0DB	Vulnerable; first fixed in 12.4 Releases up to and including 12.0(1)DB are not vulnerable.	12.4(25b) 12.4(23b)
12.0DC	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0S	12.0(32)S14; Available on 25-SEP-2009 12.0(33)S5	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(25b) 12.4(23b)
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)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	Vulnerable; first fixed in 12.0S	12.0(33)S5 12.0(32)S14; Available on 25-SEP-2009
12.0T	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.0W	Vulnerable; first fixed in 12.4 Releases up to and including 12.0(16)W5(21c) are not vulnerable.	12.4(25b) 12.4(23b)
12.0WC	Releases prior to 12.0(5)WC3b are vulnerable, release 12.0(5)WC3b and later are not vulnerable	
12.0WT	Not Vulnerable	
12.0XA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XB	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XC	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XD	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XE	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XF	Not Vulnerable	
12.0XG	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.0XH	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XI	Releases prior to 12.0(4)XI2 are vulnerable, release 12.0(4)XI2 and later are not vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XJ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XK	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XL	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XM	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XN	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XQ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XR	Vulnerable; first fixed in 12.4 Releases up to and including 12.0(6)XR are not vulnerable.	12.4(25b) 12.4(23b)

12.0XS	Not Vulnerable	
12.0XT	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.0XV	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
12.1	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1AA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1AX	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.1AY	Releases up to and including 12.1(13)AY are not vulnerable. Releases 12.1(22)AY1 and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.1AZ	Not Vulnerable	

12.1CX	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1DA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1DB	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1DC	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1E	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF17; Available on 30-SEP-2009
12.1EA	Releases up to and including 12.1(4)EA1c are not vulnerable. Releases 12.1(22)EA11 and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3
12.1EB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1EC	Vulnerable; first fixed in 12.3BC	12.2(33)SCB4 12.3(21a)BC9

12.1EO	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1EU	Vulnerable; first fixed in 12.2SG	12.2(31)SGA11; Available on 04-DEC-2009 12.2(50)SG4
12.1EV	Not Vulnerable	
12.1EW	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1EX	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1EY	Releases up to and including 12.1(1)EY are not vulnerable.	
12.1EZ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1GA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1GB	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

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

12.1XL	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XM	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XP	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XQ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XR	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XS	Vulnerable; first fixed in 12.4 Releases up to and including 12.1(1)XS are not vulnerable.	12.4(25b) 12.4(23b)
12.1XT	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XU	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XV	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XW	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.1XX	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1XY	Vulnerable; first fixed in 12.4 Releases up to and including 12.1(4)XY are not vulnerable.	12.4(25b) 12.4(23b)
12.1XZ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1YA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1YB	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1YC	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1YD	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1YE	Releases prior to 12.1(5)YE6 are vulnerable, release 12.1(5)YE6 and later are not vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1YF	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.1YH	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.1YI	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.1YJ	Not Vulnerable	
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
12.2	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2B	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2BC	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2BW	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2BX	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2BY	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.2BZ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2CX	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2CY	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2CZ	Vulnerable; first fixed in 12.2SB	12.2(31)SB16 12.2(33)SB7
12.2DA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2DD	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2DX	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2EW	Vulnerable; first fixed in 12.2SG	12.2(31)SGA11; Available on 04-DEC-2009 12.2(50)SG4
12.2EWA	Vulnerable; first fixed in 12.2SG	12.2(31)SGA11; Available on 04-DEC-2009 12.2(50)SG4
12.2EX	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009

12.2EY	Releases prior to 12.2(46)EY are vulnerable, release 12.2(46)EY and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2EZ	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2IRA	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRB	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2IXA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2IXE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXG	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXH	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2JA	Releases up to and including 12.2(13)JA4 are not vulnerable.	
12.2JK	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2MB	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2MC	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2S	Vulnerable; first fixed in 12.2SB	12.2(31)SB16 12.2(33)SB7
12.2SB	12.2(31)SB16 12.2(33)SB6 12.2(28)SB14; Available on 20-OCT-2009	12.2(33)SB7
12.2SBC	Vulnerable; first fixed in 12.2SB	12.2(31)SB16 12.2(33)SB7
12.2SCA	Vulnerable; first fixed in 12.2SCB	12.2(33)SCB4
12.2SCB	12.2(33)SCB4	12.2(33)SCB4
12.2SE	12.2(50)SE2 12.2(52)SE; Available on 13-OCT-2009	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009

12.2SEA	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SEB	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SEC	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SED	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SEE	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SEF	Releases prior to 12.2(25)SEF2 are vulnerable, release 12.2(25)SEF2 and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009

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(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SG	12.2(50)SG4 12.2(53)SG	12.2(50)SG4
12.2SGA	12.2(31)SGA11; Available on 04-DEC-2009	12.2(31)SGA11; Available on 04-DEC-2009
12.2SL	Not Vulnerable	
12.2SM	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SO	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2SQ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SRA	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2SRB	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2SRC	12.2(33)SRC5; Available on 29-OCT-2009	12.2(33)SRD3
12.2SRD	12.2(33)SRD2	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(25b) 12.4(23b)

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	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
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; first fixed in 12.2SXF	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXA	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXB	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXD	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXE	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF17; Available on 30-SEP-2009

12.2SXF	12.2(18)SXF17; Available on 30-SEP-2009 Please see IOS Software Modularity Patch	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXH	12.2(33)SXH6; Available on 30-OCT-2009 Please see IOS Software Modularity Patch	12.2(33)SXH6; Available on 30-OCT-2009
12.2SXI	12.2(33)SXI2	12.2(33)SXI2a
12.2SY	Vulnerable; first fixed in 12.2SB	12.2(31)SB16 12.2(33)SB7
12.2SZ	Vulnerable; first fixed in 12.2SB	12.2(31)SB16 12.2(33)SB7
12.2T	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
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 Releases up to and including 12.2(1)XA are not vulnerable.	12.4(25b) 12.4(23b)
12.2XB	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XC	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XD	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XE	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XF	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XG	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XH	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XI	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XJ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.2XK	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XL	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XM	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XNA	Not Vulnerable	
12.2XNB	Not Vulnerable	
12.2XNC	Not Vulnerable	
12.2XND	Not Vulnerable	
12.2XO	Vulnerable; first fixed in 12.2SG	12.2(31)SGA11; Available on 04-DEC-2009 12.2(50)SG4
12.2XQ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XR	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XS	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2XT	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

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

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

12.2YN	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YO	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YP	Vulnerable; first fixed in 12.4 Releases up to and including 12.2(8)YP are not vulnerable.	12.4(25b) 12.4(23b)
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	Not Vulnerable	
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; first fixed in 12.2SXF	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(25b) 12.4(23b)
12.2ZF	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2ZG	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.2ZH	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
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	
12.2ZP	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZU	Vulnerable; first fixed in 12.2SXH	12.2(33)SXH6; Available on 30-OCT-2009
12.2ZX	Vulnerable; first fixed in 12.2SB	12.2(31)SB16 12.2(33)SB7

12.2ZY	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZYA	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(21a)BC9
12.3BW	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3EU	Not Vulnerable	
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	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(25b) 12.4(23b)
12.3JL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.3JX	Not Vulnerable	
12.3T	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
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
12.3XA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
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(25b) 12.4(23b)

12.3XD	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XE	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
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(25b) 12.4(23b)
12.3XI	Vulnerable; first fixed in 12.2SB	12.2(31)SB16 12.2(33)SB7
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(25b) 12.4(23b)
12.3XL	Vulnerable; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3XQ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.3XR	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XS	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
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(25b) 12.4(23b)
12.3XY	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XZ	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3YA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

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	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
12.3YQ	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

12.3YS	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	Vulnerable; first fixed in 12.4XR	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(23b) 12.4(25b)	12.4(25b) 12.4(23b)
12.4GC	Not Vulnerable	
12.4JA	12.4(13d)JA	
12.4JDA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4JDC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.4JDD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4JK	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4JL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
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	Vulnerable; first fixed in 12.4JA	
12.4MD	12.4(11)MD9	12.4(11)MD9 12.4(15)MD3 12.4(22)MD1
12.4MDA	12.4(22)MDA1	12.4(22)MDA1
12.4MR	Releases prior to 12.4(19)MR3 are vulnerable, release 12.4(19)MR3 and later are not vulnerable	12.4(19)MR3
12.4SW	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

12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T2 12.4(24)T2; Available on 23-OCT-2009	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	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
12.4XE	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
12.4XF	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	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

12.4XJ	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	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.4XM	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

12.4XN	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	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
12.4XR	12.4(22)XR 12.4(15)XR6	12.4(15)XR7 12.4(22)XR
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	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
12.4XY	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
12.4XZ	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

12.4YA	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
12.4YB	12.4(22)YB4	12.4(22)YB4
12.4YD	12.4(22)YD1	12.4(22)YD1
12.4YE	12.4(22)YE1	12.4(22)YE1

Cisco IOS Software Modularity - Maintenance Packs

Customers who are using Cisco IOS Software Modularity can apply the respective maintenance packs. More information on Cisco IOS Software Modularity can be found at the following link: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd80313e15.html

The Maintenance Packs listed below can be downloaded at <http://www.cisco.com/go/pn>

Cisco IOS Software Modularity Maintenance Pack for 12.2SXF

Cisco IOS Software Release	Solution Maintenance Pack (MP)
12.2(18)SXF14	MP001
12.2(18)SXF15	MP001
12.2(18)SXF16	MP001

Cisco IOS Software Modularity Maintenance Pack for 12.2SXH

Cisco IOS Software Release	Solution Maintenance Pack (MP)
12.2(33)SXH5	MP001

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

Workarounds

Disabling Cisco Express Forwarding will mitigate this vulnerability. It can be disabled in two ways:

Disabling Cisco Express Forwarding Globally

Cisco Express Forwarding can be globally disabled by using the **no ip cef** and **no ipv6 cef** global configuration commands.

Disabling Cisco Express Forwarding on Tunnel Interfaces

Cisco Express Forwarding can also be disabled on individual tunnel interfaces. To be effective, it must be disabled on all tunnel interfaces configured on an affected device. Cisco Express Forwarding can be disabled on individual interfaces as shown in the following example:

```
interface Tunnel [interface-ID]
  no ip route-cache cef
  no ipv6 cef
```

Note: Disabling Cisco Express Forwarding may have significant performance impact and is not recommended.

Additional mitigations that can be deployed on Cisco devices in 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-20090923-tunnels.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 internally.

[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-20090923-tunnels.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-Oct-19	Updated ION software table.
Revision 1.2	2009-Oct-02	Added the availability for 12.2(31)SGA11. Configuration commands in the Workarounds section have been clarified.
Revision 1.1	2009-Sept-30	In the Workarounds section, configuration commands for disabling IPv6 CEF were added.
Revision 1.0	2009-Sept-23	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](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)