

# Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability

Advisory ID: [cisco-sa-20090923-sip](#)

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

## Revision 1.0

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

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS<sup>®</sup> Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled.

Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.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](http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html)

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

## ☐ Affected Products

This vulnerability only affects devices running Cisco IOS Software with SIP voice services enabled.

## ☐ Vulnerable Products

Cisco devices running affected Cisco IOS Software versions that are configured to process SIP messages with the Cisco Unified Border Element feature are affected. Cisco IOS devices that are not configured for SIP and Cisco Unified Border Element feature are not affected by this vulnerability.

**Note:** Cisco Unified Border Element feature (previously known as the Cisco Multiservice IP-to-IP Gateway) is a special Cisco IOS Software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

Cisco Unified Border Element feature requires the **voice service voip** command and the **allow-connections** subcommand. An example of an affected configuration is as follows:

```
voice service voip
  allow-connections from-type to to-type
...
```

Recent versions of Cisco IOS Software do not process SIP messages by default. Creating a dial peer by issuing the command **dial-peer voice** will start the SIP processes, causing the Cisco IOS device to process SIP messages. In addition, several features within Cisco Unified Communications Manager Express, such as ePhones, once configured will also automatically start the SIP process, which will cause the device to start processing SIP messages. An example of an affected configuration is as follows:

```
dial-peer voice <Voice dial-peer tag> voip
!
```

In addition to inspecting the Cisco IOS device configuration for a dial-peer command that causes the device to process SIP messages, administrators can also use the command `show processes | include SIP` to determine whether Cisco IOS Software is running the processes that handle SIP messages. In the following example, the presence of the processes **CCSIP\_UDP\_SOCKET** or **CCSIP\_TCP\_SOCKET** indicates that the Cisco IOS device is processing SIP messages:

```
Router#show processes | include SIP
 149 Mwe 40F48254          4          1      400023108/24000  0
CCSIP_UDP_SOCKET
 150 Mwe 40F48034          4          1      400023388/24000  0
CCSIP_TCP_SOCKET
```



**Warning:** Since there are several ways a device running Cisco IOS Software can start processing SIP messages, it is recommended that the **show processes | include SIP** command be used to determine whether the device is processing SIP messages instead of relying on the presence of specific configuration commands.

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

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (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>

## ☐ Products Confirmed Not Vulnerable

The SIP Application Layer Gateway (ALG), which is used by the Cisco IOS NAT and firewall features of Cisco IOS Software, is not affected by this vulnerability. Cisco IOS XE Software and Cisco IOS XR Software are not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

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

## ☐ Details

SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

The Cisco Unified Border Element (previously known as the Cisco Multiservice IP-to-IP Gateway) is a special Cisco IOS Software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

For more information about Cisco Unified Border Element refer to the following link:

<http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html>

A DoS vulnerability exists in the SIP implementation in Cisco IOS Software when devices are running a Cisco IOS image that contains the Cisco Unified Border Element feature. This vulnerability is triggered by processing a series of crafted SIP messages.

This vulnerability is documented in Cisco Bug ID [CSCsx25880](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-2870.

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

## ▣ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

<b>CSCsx25880 - Crafted SIP packet may cause device reload</b>					
<b>Calculate the environmental score of <a href="#">CSCsx25880</a></b>					
CVSS Base Score - <b>7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - <b>6.4</b>					

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

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

## ☐ Impact

Successful exploitation of the vulnerability described in this document may result in a reload of the device. The issue could be repeatedly exploited to cause an extended DoS condition.

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

## ☐ Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Each row of the Cisco IOS Software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases.		
Affected 12.1-Based	First Fixed Release	Recommended Release

<b>Releases</b>		
There are no affected 12.1 based releases.		
<b>Affected 12.2- Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.2 based releases.		
<b>Affected 12.3- Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.3	Not Vulnerable	
12.3B	Not Vulnerable	
12.3BC	Not Vulnerable	
12.3BW	Not Vulnerable	
12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	

12.3JEC	Not Vulnerable	
12.3JK	Not Vulnerable	
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	
12.3T	Not Vulnerable	
12.3TPC	Not Vulnerable	
12.3VA	Not Vulnerable	
12.3XA	Not Vulnerable	
12.3XB	Not Vulnerable	
12.3XC	Not Vulnerable	
12.3XD	Not Vulnerable	
12.3XE	Not Vulnerable	

12.3XF	Not Vulnerable	
12.3XG	Not Vulnerable	
12.3XI	Not Vulnerable	
12.3XJ	Not Vulnerable	
12.3XK	Not Vulnerable	
12.3XL	Not Vulnerable	
12.3XQ	Not Vulnerable	
12.3XR	Not Vulnerable	
12.3XS	Not Vulnerable	
12.3XU	Not Vulnerable	
12.3XW	Not Vulnerable	
12.3XX	Not Vulnerable	
12.3XY	Not Vulnerable	

12.3XZ	Not Vulnerable	
12.3YA	Not Vulnerable	
12.3YD	Not Vulnerable	
12.3YF	Not Vulnerable	
12.3YG	Not Vulnerable	
12.3YH	Not Vulnerable	
12.3YI	Not Vulnerable	
12.3YJ	Not Vulnerable	
12.3YK	Releases prior to 12.3(11)YK3 are vulnerable, release 12.3(11)YK3 and later are not vulnerable; first fixed in <a href="#">1.2.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YM	Not Vulnerable	
12.3YQ	Not Vulnerable	

12.3YS	Vulnerable; first fixed in <a href="#">12.4T</a> Releases up to and including 12.3(11)YS1 are not vulnerable.	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 <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YU	Not Vulnerable	
12.3YX	Not Vulnerable	
12.3YZ	Not Vulnerable	
12.3ZA	Not Vulnerable	
<b>Affected 12.4- Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	Not Vulnerable	
12.4GC	12.4(24)GC1	

12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JDC	Not Vulnerable	
12.4JDD	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MDA	Not Vulnerable	
12.4MR	12.4(19)MR3	12.4(19)MR3
12.4SW	Not Vulnerable	

12.4T	12.4(24)T1 12.4(15)T10 12.4(20)T3 12.4(22)T2	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 <a href="#">12.4T</a>	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 <a href="#">12.4T</a>	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 <a href="#">12.4T</a>	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 <a href="#">12.4T</a>	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 <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XK	Not Vulnerable	
12.4XL	12.4(15)XL5	
12.4XM	Vulnerable; first fixed in <a href="#">12.4T</a> Releases up to and including 12.4(15)XM are not vulnerable.	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.4XN	Not Vulnerable	
12.4XP	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Vulnerable; first fixed in <a href="#">12.4T</a>	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 <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.4XW	Vulnerable; first fixed in <a href="#">12.4T</a>	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 <a href="#">12.4T</a>	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 <a href="#">12.4T</a>	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 <a href="#">12.4T</a>	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)YB1	12.4(22)YB4
12.4YD	Not Vulnerable	
12.4YE	Not Vulnerable	

**Note:** No Cisco IOS-XE or Cisco IOS Software Modularity releases are affected by this vulnerability.

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

## ☐ Workarounds

If the affected Cisco IOS device requires SIP for VoIP services, SIP cannot be disabled, and therefore, no workarounds are available. Users are advised to apply mitigation techniques to help limit exposure to the vulnerability. Mitigation consists of allowing only legitimate devices to connect to the routers. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service

Vulnerabilities in Cisco Unified Communications Manager and Cisco IOS Software", which is available at the following location: <http://www.cisco.com/warp/public/707/cisco-amb-20090923-voice.shtml>.

## Disable SIP Listening Ports

For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to accomplish this with the following commands:

```
sip-ua
no transport udp
no transport tcp
no transport tcp tls
```



**Warning:** When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

The **show udp connections**, **show tcp brief all**, and **show processes | include SIP** commands can be used to confirm that the SIP UDP and TCP ports are closed after applying this workaround.

Depending on the Cisco IOS Software version in use, the output of "show ip sockets" still showed UDP port 5060 open, but sending something to that port caused the SIP process to emit the following message:

```
*Feb 2 11:36:47.691: sip_udp_sock_process_read: SIP UDP Listener is
DISABLED
```

## Control Plane Policing

For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to the network

```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature.) If the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.

access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061

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

```
class-map match-all drop-sip-class
  match access-group 100

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

policy-map drop-sip-traffic
  class drop-sip-class
  drop

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

control-plane
  service-policy input drop-sip-traffic
```



**Warning:** Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of the sender, which may defeat access control lists that permit communication to these ports from trusted IP addresses.

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Additional information on the configuration and use of the CoPP feature can be found at [http://www.cisco.com/web/about/security/intelligence/coppwp\\_gs.html](http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html) and [http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t4/feature/guide/gtrtlmt.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html).

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

## ☐ Obtaining Fixed Software

Cisco has released free software updates that address this vulnerability. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at [http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\\_.htm](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.htm), 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](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 discovered during internal testing.

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

## ☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

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

## ☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

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

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

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

## ☐ Revision History

Revision 1.0	2009-September-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](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)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

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