

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Security Advisories

# Cisco Security Advisory: Multiple Cisco IOS Session Initiation Protocol Denial of Service Vulnerabilities

Advisory ID: [cisco-sa-20080924-sip](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>

## Revision 1.1

Last Updated 2009 April 16 2100 UTC (GMT)

For Public Release 2008 September 24 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

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

**Note:** The September 24, 2008 IOS Advisory bundled publication includes twelve Security Advisories. Eleven of the advisories address vulnerabilities in Cisco's IOS software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each Advisory lists the releases that correct the vulnerability described in the Advisory.

Individual publication links are listed below:

- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ubr.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml>

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

## ☐ Affected Products

These vulnerabilities only affect devices running Cisco IOS that have SIP voice services enabled.

### ☐ Vulnerable Products

Cisco devices running affected Cisco IOS versions and that may process SIP messages are affected. The only requirement for these vulnerabilities is that the Cisco IOS device processes SIP messages as part of configured voice over IP (VoIP) functionality (this does not apply to processing of SIP messages as part of the NAT and firewall feature sets.) Recent versions of Cisco IOS do not process SIP messages by default, but creating a "dial peer" via the command **dial-peer voice** will start the SIP processes and cause Cisco IOS to start processing SIP messages. An example of an affected configuration is as follows:

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

Note that older versions of Cisco IOS were affected by a bug that caused Cisco IOS to process

SIP messages even without being configured for SIP operation. Please refer to <http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml> for additional information on Cisco bug ID [CSCsb25337](#) ( [registered](#) customers only) .

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 some **show** commands to determine if the Cisco IOS device is running processes that handle SIP messages, or if the device is listening on the SIP ports.

The command **show processes | include SIP** can be used to determine whether Cisco IOS is running the processes that handle SIP messages. In the following example, the presence of the processes **CCSIP\_UDP\_SOCKET** and **CCSIP\_TCP\_SOCKET** indicates that the Cisco IOS device is processing SIP messages:

```
Router#show processes | include SIP
 147 Mwe 40F46DF4          12          2      600023468/24000  0 CCSIP_SPI
 148 Mwe 40F21244          0           1           0 5524/6000      0 CCSIP_DNS
 149 Mwe 40F48254          4           1      400023108/24000  0 CCSIP_UDP
 150 Mwe 40F48034          4           1      400023388/24000  0 CCSIP_TCP
```

Different versions of Cisco IOS have different ways of verifying whether the Cisco IOS device is listening for SIP messages. The **show ip sockets**, **show udp**, **show tcp brief all**, and **show control-plane host open-ports** commands can be used to determine this, although not all of these commands work on all IOS releases. Since it is not practical in this document to provide a list of commands corresponding to the various releases, users should try the aforementioned commands to determine which ones work for their device. The following is one example of one command that shows a router listening on port 5060 (the SIP port):

```
router#show control-plane host open-ports
Active internet connections (servers and established)
Prot      Local Address      Foreign Address      Service
<output removed for brevity>
tcp              *:5060              *:0                  SIP
<output removed for brevity>
udp              *:5060              *:0                  SIP
```

In order to determine the software that runs on a Cisco IOS product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS software identifies itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name displays between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices do not have the **show version** command or give different output.

The following example shows output from a device that runs an IOS image:

```
router>show version
Cisco IOS Software, 7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(6)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 16-May-06 16:09 by kellythw
<more output removed for brevity>
```

Additional information on the Cisco IOS release naming conventions can be found on the document entitled "White Paper: Cisco IOS Reference Guide", which is available at

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

Cisco Unified Communications Manager is also affected by some of these vulnerabilities, although they are tracked by different Cisco bug IDs. A companion security advisory for Cisco Unified Communications Manager is available at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>.

## ☐ Products Confirmed Not Vulnerable

The SIP Application Layer Gateway (ALG), which is used by the IOS Network Address Translation (NAT) and firewall features of Cisco IOS, is not affected by these vulnerabilities.

Cisco devices that are running Cisco IOS XR are not affected.

With the exception of the Cisco Unified Communications Manager, no other Cisco products are currently known to be vulnerable to the issues described in this advisory.

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

## ☐ Details

SIP is a popular signaling protocol 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 is flexible to accommodate for 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.

Multiple denial of service vulnerabilities exist in the SIP implementation in Cisco IOS. In all cases vulnerabilities can be triggered by processing valid SIP messages.

### Memory Leak Vulnerability

[CSCse56800](#) ( [registered](#) customers only) causes a memory leak in affected devices. The memory leak is caused by the processing of a specific type of valid SIP messages and may eventually disrupt the availability of all voice services, even if the Cisco IOS device is still running. This vulnerability has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2008-3799.

### Device Reload Vulnerabilities

The following vulnerabilities can lead to a reload of the Cisco IOS device while processing some specific and valid SIP messages:

- [CSCsg91306](#) ( [registered](#) customers only) , assigned CVE ID CVE-2008-3800
- [CSCsl62609](#) ( [registered](#) customers only) , assigned CVE ID CVE-2008-3801
- [CSCsk42759](#) ( [registered](#) customers only) , assigned CVE ID CVE-2008-3802

[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>.

<a href="#">CSCse56800</a>					
Calculate the environmental score of <a href="#">CSCse56800</a>					
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	

<a href="#">CSCsg91306</a> , <a href="#">CSCsk42759</a> , <a href="#">CSCsl62609</a>					
Calculate the environmental score of <a href="#">CSCsg91306/CSCsk42759/CSCsl62609</a>					
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 vulnerabilities described in this document may result in a reload of the device. The issue could be repeatedly exploited to result in an extended Denial Of Service (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	
<b>Affected 12.0-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.0 based releases		
<b>Affected 12.1-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</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>
12.2	Not Vulnerable	

12.2B	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2BC	Not Vulnerable	
12.2BW	Not Vulnerable	
12.2BX	Vulnerable; first fixed in <a href="#">12.4</a>	12.2(33)SB2; Available on 26-SEP-08 12.4(15)T7 12.4(18c)
12.2BY	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Vulnerable; migrate to any release in 12.2S	12.2(33)SB2; Available on 26-SEP-08
12.2DA	Not Vulnerable	
12.2DD	Not Vulnerable	
12.2DX	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	
12.2EX	Not Vulnerable	
12.2EY	Not Vulnerable	
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Not Vulnerable	
12.2IRB	Not Vulnerable	
12.2IXA	Not Vulnerable	
12.2IXB	Not Vulnerable	
12.2IXC	Not Vulnerable	
12.2IXD	Not Vulnerable	

12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2IXG	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Releases prior to 12.2 (15)MC2c are vulnerable, release 12.2 (15)MC2c and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2S	Not Vulnerable	
12.2SB	Not Vulnerable	
12.2SBC	Not Vulnerable	
12.2SCA	Not Vulnerable	
12.2SE	Not Vulnerable	
12.2SEA	Not Vulnerable	
12.2SEB	Not Vulnerable	
12.2SEC	Not Vulnerable	
12.2SED	Not Vulnerable	
12.2SEE	Not Vulnerable	
12.2SEF	Not Vulnerable	
12.2SEG	Not Vulnerable	
12.2SG	Not Vulnerable	
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SRA	Not Vulnerable	
12.2SRB	Not Vulnerable	
12.2SRC	Not Vulnerable	
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	

12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Not Vulnerable	
12.2SXE	Not Vulnerable	
12.2SXF	Not Vulnerable	
12.2SXH	Not Vulnerable	
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2TPC	Vulnerable; contact TAC	
12.2XA	Not Vulnerable	
12.2XB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2XC	Not Vulnerable	
12.2XD	Not Vulnerable	
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	
12.2XG	Not Vulnerable	
12.2XH	Not Vulnerable	
12.2XI	Not Vulnerable	
12.2XJ	Not Vulnerable	
12.2XK	Not Vulnerable	
12.2XL	Not Vulnerable	
12.2XM	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2XN	Not Vulnerable	
12.2XNA	Not Vulnerable	

12.2XNB	Not Vulnerable	
12.2XO	Not Vulnerable	
12.2XQ	Not Vulnerable	
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2XU	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2XV	Not Vulnerable	
12.2XW	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2YA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2YB	Vulnerable; contact TAC	
12.2YC	Vulnerable; contact TAC	
12.2YD	Vulnerable; contact TAC	
12.2YE	Not Vulnerable	
12.2YF	Vulnerable; contact TAC	
12.2YG	Not Vulnerable	
12.2YH	Vulnerable; contact TAC	
12.2YJ	Vulnerable; contact TAC	
12.2YK	Not Vulnerable	
12.2YL	Vulnerable; contact TAC	
12.2YM	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
	Vulnerable; contact	

12.2YN	TAC	
12.2YO	Not Vulnerable	
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	
12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Vulnerable; contact TAC	
12.2YU	Vulnerable; contact TAC	
12.2YV	Releases prior to 12.2(11)YV1 are vulnerable, release 12.2(11)YV1 and later are not vulnerable;	
12.2YW	Vulnerable; contact TAC	
12.2YX	Not Vulnerable	
12.2YY	Vulnerable; contact TAC	
12.2YZ	Not Vulnerable	
12.2ZA	Not Vulnerable	
12.2ZB	Vulnerable; contact TAC	
12.2ZC	Vulnerable; contact TAC	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2ZF	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2ZG	Not Vulnerable	
12.2ZH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.2ZJ	Vulnerable; contact	

	TAC	
12.2ZL	Vulnerable; contact TAC	
12.2ZP	Vulnerable; contact TAC	
12.2ZU	Not Vulnerable	
12.2ZX	Not Vulnerable	
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.3	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3B	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
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	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3TPC	Vulnerable; contact TAC	
12.3VA	Vulnerable; contact TAC	
12.3XA	Releases prior to 12.3(2)XA7 are vulnerable, release 12.3(2)XA7 and	12.4(15)T7

	later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(18c)
12.3XB	Vulnerable; contact TAC	
12.3XC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XF	Vulnerable; contact TAC	
12.3XG	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XI	Vulnerable; migrate to any release in 12.2SB	12.2(33)SB2; Available on 26- SEP-08
12.3XJ	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX13 12.4(15)T7
12.3XK	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XQ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XR	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XS	Not Vulnerable	
12.3XU	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.3XW	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX13 12.4(15)T7

12.3XX	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XY	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3XZ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(15)T7 12.4(18c)
12.3YA	Not Vulnerable	
12.3YD	Not Vulnerable	
12.3YF	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX13 12.4(15)T7
12.3YG	12.3(8)YG7; Available on 01-OCT-08	12.4(15)T7
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="#">12.4T</a>	12.4(15)T7
12.3YM	12.3(14)YM13; Available on 30-SEP-08	12.3(14)YM13; Available on 30-SEP-08
12.3YQ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.3YS	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.3YT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.3YU	Vulnerable; first fixed in <a href="#">12.4XB</a>	12.4(2)XB10 12.4(9)XG3 12.4(15)T7
12.3YX	12.3(14)YX12	12.3(14)YX13
12.3YZ	12.3(11)YZ3	

12.3ZA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
<b>Affected 12.4-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	12.4(13f) 12.4(17b) 12.4(18)	12.4(18c)
12.4JA	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JMC	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	12.4(19)MR	12.4(19)MR
12.4SW	Not Vulnerable	
12.4T	12.4(15)T4 12.4(20)T 12.4(6)T11	12.4(15)T7
12.4XA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XB	12.4(2)XB10	12.4(2)XB10
12.4XC	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XD	12.4(4)XD11; Available on 26-SEP-08	12.4(4)XD11; Available on 26-SEP-08
12.4XE	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7

12.4XK	Not Vulnerable	
12.4XL	12.4(15)XL2	12.4(15)XL2
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Vulnerable; contact TAC	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XV	Vulnerable; contact TAC	
12.4XW	12.4(11)XW7	12.4(11)XW9
12.4XY	12.4(15)XY3	12.4(15)XY4
12.4XZ	Not Vulnerable	
12.4YA	Not Vulnerable	

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

## ☐ Workarounds

If the affected Cisco IOS device needs to provide voice over IP services and therefore SIP cannot be disabled then none of the listed vulnerabilities have workarounds. Users are advised to apply mitigation techniques to limit exposure to the listed vulnerabilities. Mitigation consists of only allowing 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 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-20080924-sip.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 allow administrators to accomplish this with the following commands:

```

sip-ua
  no transport udp
  no transport tcp

```



**Warning:** When applying this workaround to devices processing MGCP or H.323 calls, the device will not allow you to 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.

It is recommended that after applying this workaround, the **show** commands discussed in the Vulnerable Products section be used to confirm that the Cisco IOS device is no longer processing SIP messages.

## 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 software 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 your 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 utilize UDP as a transport protocol, it is possible to easily spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Additional information on the configuration and use of the CoPP feature can be found at

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod\\_white\\_paper0900](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900); and [http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t4/feature/guide/gtrtlimt.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html).

[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](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](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto: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](mailto: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/warp/public/687/Directory/DirTAC.shtml> 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.

These vulnerabilities were discovered by Cisco internal testing and during handling of customer service requests.

[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-20080924-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 1.1	2009-April-16	Removed references to the combined software table, as it is now outdated
Revision 1.0	2008-September-24	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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)