

Cisco Security Advisory: Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability

Advisory ID: cisco-sa-20090325-udp

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

Revision 1.5

Last Updated 2009 June 26 1500 UTC (GMT)

For Public Release 2009 March 25 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

- [Summary](#)
 - [Affected Products](#)
 - [Details](#)
 - [Vulnerability Scoring Details](#)
 - [Impact](#)
 - [Software Versions and Fixes](#)
 - [Workarounds](#)
 - [Obtaining Fixed Software](#)
 - [Exploitation and Public Announcements](#)
 - [Status of this Notice: FINAL](#)
 - [Distribution](#)
 - [Revision History](#)
 - [Cisco Security Procedures](#)
-

Summary

Several features within Cisco IOS Software are affected by a crafted UDP packet

vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at the following link:

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

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory.

Individual publication links are listed below:

- Cisco IOS cTCP Denial of Service Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>
- Cisco IOS Software Multiple Features IP Sockets Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>
- Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>
- Cisco IOS Software Secure Copy Privilege Escalation Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>
- Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml>
- Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml>
- Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>
- Cisco IOS Software WebVPN and SSLVPN Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

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

☐ Affected Products

☐ Vulnerable Products

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

- IP Service Level Agreements (SLA) Responder
- Session Initiation Protocol (SIP)

- H.323 Annex E Call Signaling Transport
- Media Gateway Control Protocol (MGCP)

Details on how to see if the affected feature is enabled on a device, is provided within the details section of this advisory.

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

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

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), REI
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link: <http://www.cisco.com/warp/public/620/1.html>.

▣ Products Confirmed Not Vulnerable

The following products and features are not affected by this vulnerability:

- Cisco IOS XR Software
- Service Assurance Agent (SAA)
- Response Time Reporter (RTR)

- Cisco 500 Series Wireless Express Access Points
- Cisco Aironet 1250 Series
- Cisco Aironet 1240 AG Series
- Cisco Aironet 1230 AG Series
- Cisco Aironet 1200 Series
- Cisco Aironet 1140 Series
- Cisco Aironet 1130 AG Series
- Cisco Aironet 1100 Series
- Cisco Aironet 1500 Series
- Cisco Aironet 1400 Series
- Cisco Aironet 1300 Series
- Cisco AP801 (in 860 and 880 series ISRs)
- Cisco WMIC (in Cisco 3200 MARs)
- No other feature or protocol on Cisco IOS is known to be affected

No other Cisco products are currently known to be affected by this vulnerability.

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

▣ Details

A device is vulnerable if any of the features outlined below is configured and their associated UDP port number accessible. For each feature, in addition to inspecting the Cisco IOS device for vulnerable configurations, administrators can also use some show commands to determine if the Cisco IOS device is running processes that handle the UDP service, or if the device is listening on the affected UDP ports.

Different versions of Cisco IOS Software have different methods of showing the UDP ports on which the Cisco IOS Software device is listening. The "**show ip sockets**" or "**show udp**" commands can be used to determine these ports. For each feature, one example is given using the above commands to show the affected UDP port number.

Successful exploitation of this vulnerability can block an interface on the device. The interface type is not relevant for this vulnerability so all Ethernet based interfaces, ATM, Serial, POS and other types of interfaces can be affected. All defined sub interfaces under a main physical interface are affected if the main interface is blocked. If the attack originates over a sub interface, the main interface will block. A blocked interface will stop receiving any subsequent packets until it is unblocked. All other interfaces are not affected and they will continue receiving and transmitting packets.

Only packets destined for a reachable configured IP address on any interface of the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

A symptom of this type of blocked queue is the failure of control-plane protocols such as routing protocols (OSPF, EIGRP, BGP, ISIS, etc.) and MPLS TDP/LDP to properly establish connections over an affected interface. Transit traffic may be affected once protocol timers expire on the affected device.

In order to identify a blocked input interface, issue the "**show interfaces**" command, and search for the Input Queue line. The size of the input queue can continue to increase. If the current size, which is 76 in the example below, is equal or larger than the maximum size (default being 75), the input queue may be blocked.

It is possible that a device receives a high rate of traffic destined to the control plane, and the full queue is only a transient event. In order to verify if the interface is actually blocked, shut down the interface with the shutdown interface configuration command and examine the input queue. If the input queue does not display 0 packets, the interface is blocked.

```
Router#show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
Hardware is AmdP2, address is 0050.500e.f1e0 (bia 0050.500e.
Internet address is 192.168.0.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255,
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:41, output 00:00:07, output hang never
Last clearing of "show interface" counters 00:07:18
Input queue: 76/75/1091/0 (size/max/drops/flushes); Total ou
```

IP Service Level Agreements (SLAs) Responder

Devices configured with the Cisco IOS IP Service Level Agreements (SLAs) Responder for User Datagram Protocol (UDP) echo or jitter operations feature are vulnerable. Any device configured to act as a responder is vulnerable. The following shows two different vulnerable configurations. The first being a generic IP SLA responder:

```
ip sla responder
```

or

```
ip sla monitor responder
```

The following shows this second configuration with a more specific UDP responder configured:

```
ip sla responder
ip sla responder udp-echo ipaddress 10.10.10.10 port 1025
```

Service Assurance Agent (SAA) and Response Time Reporter (RTR) feature are

"not" affected and use the **"rtr"** CLI command syntax. The following example shows a configuration, which is not vulnerable:

```
rtr responder
```

The following example shows a device listening on the default IP SLA control channel with the affected UDP port 1967.

```
Router#show udp
Proto      Remote          Port      Local          Port   In Out Stat
 17 0.0.0.0      0 10.2.6.1      1967    0  0  211
```

Further information about Cisco IOS IP SLAs is available in "Cisco IOS IP SLAs Configuration Guide, Release 12.4 - Cisco IOS IP SLAs Overview" at the following link:

http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsoverv.htm

Session Initiation Protocol (SIP)

Note: For customers with devices enabled with SIP, please also consult the document "Cisco Security Advisory: Cisco IOS Session Initiation Protocol Denial of Service Vulnerability" at the following link:

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

Cisco devices that process SIP messages are affected. Recent versions of Cisco IOS Software do not process SIP messages by default. Creating a "dial peer" via the command **"dial-peer voice"** with any option will start the SIP processes and cause Cisco IOS Software to begin processing SIP messages. Several features within Cisco Call Manager Express, such as ePhones, once configured will also automatically start the SIP process and the device will begin processing SIP messages. It is recommended if the device is running any voice configurations to confirm the existence of the SIP process with the **"show ip socket"** or **"show udp"** command. The following is one example of an affected configuration:

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

Note: Older versions of Cisco IOS Software were affected by a bug that caused Cisco IOS Software to process SIP messages even without being configured for SIP operation. Please refer to "Cisco Security Advisory: SIP Packets Reload IOS Devices with support for SIP" at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>

The following example shows a device that will process SIP messages, on the default affected UDP port 5060:

```
Router#show ip socket
Proto      Remote          Port      Local          Port   In Out Stat
```

```
17 0.0.0.0          0 192.168.0.2      5060  0  0  211
```

Further information about SIP, is available in the "Cisco IOS SIP Configuration Guide" at the following link:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c

H.323 Annex E Call Signaling Transport

Cisco devices that are configured to support H.323 are affected. The affected protocol is H.323 Annex E Call Signaling Transport over UDP. ITU-T recommendation H.323 Annex E describes the signaling framework and wire-protocol for transporting H.225.0 call signaling messages over UDP. Recent versions of Cisco IOS Software do not open H.225.0 UDP port by default. Creating a "dial-peer" via the command "**dial-peer voice**" with any option will open the H.225.0 UDP port. Several features within Cisco Call Manager Express, such as ePhones, once configured will also automatically start the H.323 process and the device will begin processing H.323 packets. It is recommended if the device is running any voice configurations to confirm the existence of the H.323 process with the "**show ip socket**" or "**show udp**" command. The following is one example of an affected configuration:

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

Note: Older versions of Cisco IOS Software were affected by a bug that caused Cisco IOS Software to listen on H.323 ports without being configured for H.323 operation. Please refer to Cisco bug ID: [CSCsb25337](#) ([registered](#) customers only)

The following example shows a device that will process H.225.0 packets, on the default affected UDP port 2517:

```
Router#show ip socket
Proto      Remote          Port          Local          Port    In Out Stat
-----
17 0.0.0.0          0 192.168.0.2      2517    0  0  211
```

Further information about H.323, is available in the "Cisco IOS H.323 Configuration Guide" at the following link:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_h323_configuration_g

Media Gateway Control Protocol (MGCP)

Devices configured with the MGCP feature are vulnerable. MGCP is enabled globally with the command "**mgcp**". The default listening port for MGCP is UDP 2427. The following example shows a vulnerable configuration:

```
mgcp
```

The following example shows a device that will process MGCP packets on the affected UDP ports:

```
Router#show ip socket
Proto    Remote      Port      Local      Port    In Out Stat
 17 192.168.0.1 2427 10.66.91.138 2427    0  0  211
```

Further information about MGCP is available in the "Configuring the Cisco IOS MGCP Gateway reference" at the following link:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186

This vulnerability is documented in the following Cisco Bug ID: [CSCsk64158](#) ([registered](#) customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifiers CVE-2009-0631.

[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>

CSCsk64158: Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability					
Calculate the environmental score of CSCsk64158					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

▣ Impact

Successful exploitation of this vulnerability may cause the inbound interface to be blocked and will silently drop any received traffic. A reload of the device is required to restore normal functionality.

[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(18e) 12.4(23a); Available on 05-JUN-2009
12.0DA	Vulnerable; first fixed in 12.2DA	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0DB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0DC	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0S	12.0(32)S12 12.0(33)S3; Available on 30-APR-2009	12.0(32)S12
12.0SC	Vulnerable; first fixed in 12.0S	12.0(32)S12
12.0SL	Vulnerable; first fixed in 12.0S	12.0(32)S12
12.0SP	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0ST	Vulnerable; first fixed in 12.0S	12.0(32)S12
12.0SX	Vulnerable; first fixed in 12.0S	12.0(32)S12
12.0SY	12.0(32)SY8	12.0(32)SY8
12.0SZ	Vulnerable; first fixed in 12.0S	12.0(32)S12

12.0T	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0W	Vulnerable; contact TAC	
12.0WC	Vulnerable; contact TAC	
12.0WT	Not Vulnerable	
12.0XA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XC	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XD	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XE	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XF	Not Vulnerable	
12.0XG	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
		12.4(18e)

12.0XH	Vulnerable; first fixed in 12.4	12.4(23a); Available on 05-JUN-2009
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(18e) 12.4(23a); Available on 05-JUN-2009
12.0XJ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XK	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XL	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XM	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XN	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XQ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XR	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a);

		Available on 05-JUN-2009
12.0XS	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XT	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XV	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
12.1	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1AA	Vulnerable; contact TAC	
12.1AX	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.1AY	Vulnerable; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
12.1AZ	Vulnerable; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
12.1CX	Vulnerable; contact TAC	
12.1DA	Vulnerable; contact TAC	
12.1DB	Vulnerable;	

	contact TAC	
12.1DC	Vulnerable; contact TAC	
12.1E	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.1EA	12.1(22)EA13	12.1(22)EA13
12.1EB	Vulnerable; contact TAC	
12.1EC	Vulnerable; first fixed in 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.1EO	Vulnerable; contact TAC	
12.1EU	Vulnerable; first fixed in 12.2SG	12.2(31)SGA9
12.1EV	Vulnerable; contact TAC	
12.1EW	Vulnerable; migrate to 12.2SGA	12.2(31)SGA9
12.1EX	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.1EY	Vulnerable; contact TAC	
12.1EZ	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.1GA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.1GB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
		12.4(18e)

12.1T	Vulnerable; first fixed in 12.4	12.4(23a); Available on 05-JUN-2009
12.1XA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XC	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XD	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XE	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XF	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XG	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XH	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009

12.1XI	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XJ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XL	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XM	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XP	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XQ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XR	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XS	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XT	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a);

		Available on 05-JUN-2009
12.1XU	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XV	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XW	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XX	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XY	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XZ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
		12.4(18e)

12.1YC	Vulnerable; first fixed in 12.4	12.4(23a); Available on 05-JUN-2009
12.1YD	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
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(18e) 12.4(23a); Available on 05-JUN-2009
12.1YF	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YH	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YI	Vulnerable; contact TAC	
12.1YJ	Vulnerable; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
12.2	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2B	Vulnerable; first	12.4(22)T1 12.4(15)T9;

	fixed in 12.4T	Available on 29-APR-2009
12.2BC	Vulnerable; migrate to 12.2SCB or 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.2BW	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2BX	Vulnerable; migrate to 12.2SB	12.2(33)SB4
12.2BY	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2BZ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2CX	Vulnerable; migrate to 12.2SCB or 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.2CY	Vulnerable; migrate to 12.2SCB or 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.2CZ	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2DA	12.2(12)DA14; Available on 30- JUL-2009	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2DD	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a);

		Available on 05-JUN-2009
12.2DX	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2EW	Vulnerable; first fixed in 12.2SG	12.2(31)SGA9
12.2EWA	Vulnerable; first fixed in 12.2SG	12.2(31)SGA9
12.2EX	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2EY	12.2(44)EY	12.2(44)SE6
12.2EZ	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2FX	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2FY	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2FZ	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2IRA	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4; Available on 18-MAY-2009
12.2IRB	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4; Available on 18-MAY-2009
12.2IXA	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2IXB	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2IXC	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009

12.2IXD	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31- MAR-2009
12.2IXE	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31- MAR-2009
12.2IXF	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31- MAR-2009
12.2IXG	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31- MAR-2009
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.2MB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2MC	12.2(15)MC2m	12.2(15)MC2m
12.2S	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2SB	12.2(31)SB14 12.2(33)SB3 12.2(28)SB13	12.2(33)SB4
12.2SBC	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2SCA	Vulnerable; first fixed in 12.2SCB	12.2(33)SCB1
12.2SCB	12.2(33)SCB1	12.2(33)SCB1
	12.2(46)SE2	

12.2SE	12.2(44)SE5 12.2(50)SE	12.2(44)SE6
12.2SEA	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEB	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEC	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SED	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEE	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEF	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEG	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SG	12.2(50)SG	12.2(52)SG; Available on 15-MAY-2009
12.2SGA	12.2(31)SGA9	12.2(31)SGA9
12.2SL	Not Vulnerable	
12.2SM	Vulnerable; contact TAC	
12.2SO	Vulnerable; contact TAC	
12.2SQ	12.2(44)SQ1	
12.2SRA	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4; Available on 18-MAY-2009
12.2SRB	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4; Available on 18-MAY-2009 12.2(33)SRB5a; Available on 3-April-2009
12.2SRC	12.2(33)SRC3	12.2(33)SRC4; Available on 18-

		MAY-2009
12.2SRD	Not Vulnerable	
12.2STE	Vulnerable; contact TAC	
12.2SU	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.2SV	Vulnerable; contact TAC	
12.2SVA	Vulnerable; contact TAC	
12.2SVC	Vulnerable; contact TAC	
12.2SVD	Vulnerable; contact TAC	
12.2SVE	Vulnerable; contact TAC	
12.2SW	Vulnerable; contact TAC	
12.2SX	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXA	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXB	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXD	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXE	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXF	12.2(18)SXF16	12.2(18)SXF16
12.2SXH	12.2(33)SXH5; Available on 20- APR-2009	12.2(33)SXH5; Available on 20- APR-2009
12.2SXI	Not Vulnerable	
12.2SY	Vulnerable; first fixed in 12.2SB	12.2(33)SB4

12.2SZ	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2T	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2TPC	Vulnerable; contact TAC	
12.2XA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XC	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XD	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XE	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XF	Vulnerable; migrate to 12.2SCB or 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.2XG	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009

12.2XH	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XI	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XJ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XK	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XL	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XM	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XN	Vulnerable; first fixed in 12.2SRC	12.2(33)SB4 12.2(33)SRD1
12.2XNA	Vulnerable; migrate to any release in 12.2SRD	12.2(33)SRD1
12.2XNB	12.2(33)XNB1	12.2(33)XNB3
12.2XNC	Not Vulnerable	
12.2XO	12.2(46)XO	12.2(46)XO
	Vulnerable; first	12.4(18e)

12.2XQ	fixed in 12.4	12.4(23a); Available on 05- JUN-2009
12.2XR	Not Vulnerable	
12.2XS	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2XT	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2XU	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2XV	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2XW	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2YA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2YB	Vulnerable; contact TAC	
12.2YC	Vulnerable; contact TAC	
12.2YD	Vulnerable; contact TAC	
12.2YE	Vulnerable; contact TAC	

12.2YF	Vulnerable; contact TAC	
12.2YG	Vulnerable; contact TAC	
12.2YH	Vulnerable; contact TAC	
12.2YJ	Vulnerable; contact TAC	
12.2YK	Vulnerable; contact TAC	
12.2YL	Vulnerable; contact TAC	
12.2YM	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.2YN	Vulnerable; contact TAC	
12.2YO	Vulnerable; contact TAC	
12.2YP	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2YQ	Vulnerable; contact TAC	
12.2YR	Vulnerable; contact TAC	
12.2YS	Not Vulnerable	
12.2YT	Vulnerable; contact TAC	
12.2YU	Vulnerable; contact TAC	
12.2YV	Vulnerable; contact TAC	
12.2YW	Vulnerable; contact TAC	

12.2YX	Vulnerable; contact TAC	
12.2YY	Vulnerable; contact TAC	
12.2YZ	Vulnerable; contact TAC	
12.2ZA	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2ZB	Vulnerable; contact TAC	
12.2ZC	Vulnerable; contact TAC	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2ZF	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.2ZG	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.2ZH	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2ZJ	Vulnerable; contact TAC	
12.2ZL	Vulnerable; contact TAC	
12.2ZP	Vulnerable; contact TAC	

12.2ZU	Vulnerable; first fixed in 12.2SXH	12.2(33)SRC4; Available on 18-MAY-2009
12.2ZX	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2ZY	Vulnerable; contact TAC	
12.2ZYA	12.2(18)ZYA1	12.2(18)ZYA1
Affected 12.3- Based Releases	First Fixed Release	Recommended Release
12.3	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3B	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3BC	12.3(23)BC6	12.3(23)BC6
12.3BW	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	
12.3JK	Not Vulnerable	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3JL	Vulnerable; contact TAC	

12.3JX	Not Vulnerable	
12.3T	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3TPC	Vulnerable; contact TAC	
12.3VA	Vulnerable; contact TAC	
12.3XA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3XB	Vulnerable; contact TAC	
12.3XC	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XD	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XE	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3XF	Vulnerable; contact TAC	
12.3XG	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XI	Vulnerable; first fixed in 12.2SB	12.2(33)SB4

12.3XJ	Vulnerable; first fixed in 12.3YX	12.3(14)YX14
12.3XK	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XL	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XQ	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XR	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3XS	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XU	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XW	Vulnerable; first fixed in 12.3YX	12.3(14)YX14
12.3XX	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XY	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-

		APR-2009
12.3XZ	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YA	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YD	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YF	Vulnerable; first fixed in 12.3YX	12.3(14)YX14
12.3YG	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YH	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YI	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YJ	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YK	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009

12.3YM	12.3(14)YM13	12.3(14)YM13
12.3YQ	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YS	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YT	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YU	Vulnerable; first fixed in 12.4XB	12.4(22)T1
12.3YX	12.3(14)YX14	12.3(14)YX14
12.3YZ	Vulnerable; contact TAC	
12.3ZA	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
Affected 12.4- Based Releases	First Fixed Release	Recommended Release
12.4	12.4(23) 12.4(18e) 12.4(23a); Available on 05-JUN-2009	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	

12.4JMA	Vulnerable; contact TAC	
12.4JMB	Vulnerable; contact TAC	
12.4JX	Not Vulnerable	
12.4MD	12.4(11)MD7	12.4(11)MD7
12.4MR	12.4(19)MR1	12.4(19)MR2
12.4SW	Vulnerable; contact TAC	
12.4T	12.4(15)T8 12.4(20)T2 12.4(22)T 12.4(15)T9; Available on 29- APR-2009	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XA	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XB	12.4(15)T8 12.4(20)T2	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XC	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XD	12.4(4)XD12; Available on 27- MAR-2009	12.4(4)XD12; Available on 27- MAR-2009
12.4XE	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
		12.4(22)T1

12.4XF	Vulnerable; first fixed in 12.4T	12.4(15)T9; Available on 29-APR-2009
12.4XG	12.4(15)T8 12.4(20)T2 12.4(22)T1	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XJ	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XK	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XL	12.4(15)XL4	12.4(15)XL4
12.4XM	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XN	Vulnerable; contact TAC	
12.4XP	Vulnerable; contact TAC	
12.4XQ	12.4(15)XQ2	12.4(15)XQ2
12.4XR	12.4(15)XR4	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XT	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XV	Vulnerable; contact TAC	

12.4XW	12.4(11)XW10	12.4(11)XW10
12.4XY	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XZ	12.4(15)XZ2	12.4(15)XZ2
12.4YA	12.4(20)YA2	12.4(20)YA3
12.4YB	Not Vulnerable	
12.4YD	Not Vulnerable	

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

Workarounds

The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Disable Affected Listening Ports

If an affected feature is not required it can be explicitly disabled. Once disabled confirm the listening UDP port has been closed by entering the CLI command "**show udp**" or "**show ip socket**". Some features may require a reload of the device after disabling the feature in order to close the listening UDP port.

For SIP it is possible to disable UDP listening if only TCP services are required. The following example shows how to disable SIP from listening on its associated UDP port.

Note: This work around will only apply to Cisco IOS Software images with Cisco Bug ID CSCsi34903 integrated.

Warning: When applying this workaround to devices that are processing MGCP or H.323 calls, the device will not allow the stopping SIP processing while active calls are being processed. When possible, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#sip-ua
Router(config-sip-ua)#no transport udp
Router(config-sip-ua)#end
```

For SIP it is possible to bind the process to a privately-addressed interface, with the

command below. This will cause SIP to only listen on the internal interface, which may assist in limiting the exposure of this vulnerability:

```
voice service voip
  sip
    bind control source-interface <int>
    bind media source-interface <int>
```

Infrastructure Access Control Lists

Warning: Because the features in this vulnerability utilize UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:

```
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---
!---
!--- Feature: IP SLAs UDP Responder
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 1967

!--- Deny IP SLAs UDP Responder traffic from all other source
!--- destined to infrastructure addresses.

access-list 150 deny udp any
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 1967

!---
!--- Feature: Session Initiation Protocol (SIP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
```

```
INFRASTRUCTURE_ADDRESSES WILDCARD eq 5060
```

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

```
access-list 150 deny udp any  
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 5060
```

```
!---  
!--- Feature: H.323 Call Signaling  
!---
```

```
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD  
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2517
```

```
!--- Deny H.323 Call Signaling traffic from all other sources  
!--- destined to infrastructure addresses.
```

```
access-list 150 deny udp any  
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2517
```

```
!---  
!--- Feature: Media Gateway Control Protocol (MGCP)  
!---
```

```
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD  
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2427
```

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

```
access-list 150 deny udp any  
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2427
```

```
!--- Permit/deny all other Layer 3 and Layer 4 traffic in  
!--- accordance with existing security policies and  
!--- configurations. Permit all other traffic to transit the  
!--- device.
```

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

```
!--- Apply access-list to all interfaces (only one example
!--- shown)
```

```
interface serial 2/0
 ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00:

Control Plane Policing

Warning: Because the features in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP which will protect all devices with IP addresses in the infrastructure IP address range.

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

```
!---
!--- Feature: IP SLAs UDP Responder
!---
```

```
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
 any eq 1967
```

```
!---
!--- Deny IP SLAs UDP Responder traffic from all other source
!--- destined to the device control plane.
!---
```

```
access-list 150 permit udp any any eq 1967
```

```
!---  
!--- Feature: Session Initiation Protocol (SIP)  
!---
```

```
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 5060
```

```
!---  
!--- Deny SIP traffic from all other sources destined  
to the device control plane.  
!---
```

```
access-list 150 permit udp any any eq 5060
```

```
!---  
!--- Feature: H.323 Call Signaling  
!---
```

```
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 2517
```

```
!---  
!--- Deny H.323 call signaling traffic from all other sources  
destined to the device control plane.  
!---
```

```
access-list 150 permit udp any any eq 2517
```

```
!---  
!--- Feature: Media Gateway Control Protocol (MGCP)  
!---
```

```
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 2427
```

```
!---  
!--- Deny MGCP traffic from all other sources destined  
to the device control plane.
```

```

!---

access-list 150 permit udp any any eq 2427

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

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

!---

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

policy-map drop-udp-traffic
  class drop-udp-class
    drop

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

control-plane
  service-policy input drop-udp-traffic

```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS trains:

```

policy-map drop-udp-traffic
  class drop-udp-class
    police 32000 1500 1500 conform-action drop exceed-action drop

```

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

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

Additional mitigations that can be deployed on Cisco devices within the network are available in the "Cisco Applied Mitigation Bulletin" companion document for this advisory at the following link: <http://www.cisco.com/warp/public/707/cisco-amb-20090325-sip-and-udp.shtml>

Exploit Detection

It is possible to detect blocked interface queues with an Cisco IOS Embedded Event Manager (EEM) policy. EEM provides event detection and reaction capabilities on a Cisco IOS device. EEM can alert administrators of blocked interfaces with email, a syslog message, or a Simple Network Management Protocol (SNMP) trap.

A sample EEM policy that uses syslog to alert administrators of blocked interfaces is available at Cisco Beyond, an online community dedicated to EEM. A sample script is available at the following link:

<http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=981>

Further information about EEM is available from Cisco.com at the following link: http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.

[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_.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 discovered by Cisco during routine internal testing.

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

☐ **Status of this Notice: FINAL**

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

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

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

☐ **Distribution**

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

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.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 1.5	2009- June-26	Removed references to the March/09 combined fixed software table.
Revision 1.4	2009- June-1	Updated expected public availability date for release 12.4(23a).
Revision 1.3	2009- May-1	Updated expected public availability date for release 12.4(23a).
Revision 1.2	2009- March- 30	Specifically called out Wireless Products as not affected
Revision 1.1	2009- March- 25	Revised procedure for disabling affected listening ports; see Workarounds .
Revision 1.0	2009- March- 25	Initial public release.

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

☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

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

Help us help you.

- **Please rate this document.**
- Excellent

- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

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