

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

Security Advisories

Cisco Security Advisory: Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager

Advisory ID: [cisco-sa-20070808-IOS-voice](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

Revision 1.2

Last Updated 2007 August 20 1500 UTC (GMT)

For Public Release 2007 August 08 1600 UTC (GMT)

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

Contents

- [Summary](#)
- [Affected Products](#)
- [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 voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the **Software Versions and Fixes** section contains fixes for all vulnerabilities mentioned 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.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The advisories all affect IOS, one additionally affects Cisco Unified Communications Manager as well. Each advisory lists the releases that correct the vulnerability described in the advisory, and the advisories also detail the releases that correct the vulnerabilities in all four advisories. Individual publication links are listed below:

- Cisco IOS Information Leakage Using IPv6 Routing Header
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml>
- Cisco IOS Next Hop Resolution Protocol Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml>
- Cisco IOS Secure Copy Authorization Bypass Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml>
- Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>
- Cisco Unified MeetingPlace XSS Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml>

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

☐ Affected Products

These vulnerabilities only affect devices running Cisco IOS that have voice services enabled. The only exception is the vulnerability documented as Cisco bug ID [CSCsi80102](#) ([registered](#) customers only), which also exists on Cisco Unified Communications Manager.

☐ Vulnerable Products

To determine the software running on a Cisco IOS product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices will not have the **show version** command, or will give different output.

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

```
Router>show version
Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(14)T1, REL
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 31-Mar-05 08:04 by yiyao
```

Additional information about Cisco IOS release naming is available at the following link:
<http://www.cisco.com/warp/public/620/1.html>.

SIP-related vulnerabilities

Any Cisco device that runs a vulnerable version of IOS and supports SIP processing could be vulnerable. This includes multiple IOS versions of 12.2, 12.3 and 12.4. Routers that are configured as SIP Public Switched Telephone Network (PSTN) Gateways and SIP Session Border Controllers (SBCs) are vulnerable. The CAT6000-CMM card is also vulnerable.

To determine if the device has SIP enabled, enter the commands **show ip sockets** and **show tcp brief all**. In some newer IOS releases the command **show ip sockets** is removed. If that is the case use **show udp**. The output is identical to the **show ip sockets** command.

```
Router#show ip sockets
Proto Remote      Port      Local      Port  In  Out  Stat  TTY  OutputIF
17 0.0.0.0          0  --any--    5060    0   0   211   0
17 0.0.0.0          0 192.168.100.2  67     0   0  2211   0
17 0.0.0.0          0 192.168.100.2 2517    0   0    11   0
```

The first line with UDP Port 5060 shows that UDP SIP is enabled.

```
Router#show tcp brief all
TCB      Local Address      Foreign Address      (state)
2051E680 *.5060              *.*                  LISTEN
```

The above lines with *.5060 show that TCP SIP is enabled.

The device is vulnerable even if it does not have SIP explicitly configured. If the output of the **show ip sockets** command is showing that the device is listening to port 5060, then the device is vulnerable.

MGCP-related vulnerabilities

To determine whether MGCP is configured on an IOS device, look for either of the following lines in in the Cisco IOS configuration:

```
Router#show running config
....
voice-port 1/1/1
!
mgcp
!
dial-peer voice 1 pots
  service mgcpapp
```

```
port 1/1/1
```

or

```
Router#show running config
....
controller T1 1/1
  framing sf
  linecode ami
  pri-group timeslots 1-24 service mgcp
```

or

```
Router#show running config
....
controller T1 1/1
  framing sf
  linecode ami
  ds0-group 0 timeslots 1-24 type none service mgcp
```

The exact port numbers may vary in the configuration.

H.323 signaling-related vulnerabilities

To determine whether H.323 is configured on an IOS device, look for either of the following lines in the Cisco IOS configuration.

For Cisco bug ID [CSCsi60004](#) ([registered](#) customers only) this configuration is vulnerable:

```
Router#show running config | include proxy
proxy h323
```

For Cisco bug ID [CSCsg70474](#) ([registered](#) customers only) this configuration is vulnerable:

```
Router#show running config | include inspect
ip inspect name H323_protocol h323
ip inspect H323_protocol in
```

Real-time Transport Protocol-related vulnerabilities

No particular configuration is required to enable RTP because this protocol is invoked when audio or video information is transmitted. H.323, MGCP, SIP, or H.320 protocols must be processing packets for a router to process RTP packets.

Note: These vulnerabilities only affect sessions terminating or originating on a device itself, not transit traffic; for example, traffic that passes through a device, but is destined elsewhere is not affected.

Facsimile reception vulnerability

The IOS device will listen to incoming facsimile transmission by default if the Digital Signal Processor (DSP) is present. To determine the presence of DSP on a device, execute the following

command:

Note: This vulnerability only affects sessions terminating or originating on a device itself, not transit traffic; for example, traffic that passes through a device, but is destined elsewhere is not affected.

```
Router#show voice dsp
  DSP   DSP
TYPE  NUM CH CODEC      DSPWARE CURR  BOOT
=====
C542  001 01 None          7.4.1  IDLE  idle
C542  002 01 None          7.4.1  IDLE  idle
RST  AI  VOICEPORT  TS  ABORT  PAC
=====
```

The above example shows that DSP is present on the device.

☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities. The following devices are known not to be affected:

- Cisco Unified Communications Manager (with the exception of [CSCsi80102](#) ([registered](#) customers only))
- Cisco IP Phone

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

☐ Details

Details for vulnerabilities are grouped by category and impact.

SIP-related vulnerabilities

SIP is a protocol that is used to establish, modify, and terminate multimedia sessions. Most commonly, SIP is used for Internet telephony. SIP call signaling can use UDP (User Datagram Protocol) or TCP (Transport Control Protocol) as an underlying transport protocol. In all cases vulnerabilities can be triggered by processing a malformed SIP packet.

A malformed SIP packet may cause a vulnerable device to crash and may allow arbitrary code to be executed. These vulnerabilities are documented as the following Cisco Bug IDs:

- [CSCsi80749 Crash while processing malformed SIP packet](#) ([registered](#) customers only)
- [CSCsi80102 CUCM - Crash while processing malformed SIP packet](#) ([registered](#) customers only)

A malformed SIP packet may cause a memory leak and device crash. These vulnerabilities are documented as the following Cisco Bug IDs:

- [CSCsf11855 Crash while processing malformed SIP packet](#) ([registered](#) customers only)
- [CSCeb21064 Crash while processing malformed SIP packet](#) ([registered](#) customers only)
- [CSCse40276 Router crashed by malformed SIP message](#) ([registered](#) customers only)
- [CSCse68355 Router crashed by malformed SIP packet](#) ([registered](#) customers only)

- [CSCsf30058 Memory leak when processing malformed SIP message](#) ([registered](#) customers only)
- [CSCsb24007 Memory corruption and unexpected reload on receiving a SIP packet](#) ([registered](#) customers only)
- [CSCsc60249 Crash while processing malformed SIP packet](#) ([registered](#) customers only)

MGCP-related vulnerabilities

MGCP is a protocol for controlling media gateways from external call control elements such as Media Gateway Controllers or Call Agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. In a Cisco environment, a media gateway is used between the Cisco Communications Manager and the Cisco router and servers as a voice gateway.

A specially crafted MGCP packet can cause a vulnerable device to crash or become unresponsive. The unresponsive device will not be able to establish new telephone calls, and a reboot is required to restore normal operation. These vulnerabilities are documented as the following Cisco Bug IDs:

- [CSCsf08998 MGCP stop responding after receiving malformed packet](#) ([registered](#) customers only)
- [CSCsd81407 Router crash on receiving abnormal MGCP messages](#) ([registered](#) customers only)

H.323-signaling related vulnerabilities

H.323 is an ITU (International Telecommunications Union) set of recommendations for multimedia communication and signaling in networks that use Internet Protocol.

A malformed H.323 packet can crash a vulnerable device. These vulnerabilities are documented as the following Cisco Bug IDs:

- [CSCsi60004 H323 Proxy Unregistration from Gatekeeper](#) ([registered](#) customers only)
- [CSCsg70474 IOS FW with h323 inspect crashes when malformed H.323 packets received](#) ([registered](#) customers only)

Real-time Transport Protocol-related vulnerabilities

RTP is a protocol that is designed to provide delivery services for data with real-time characteristics, such as interactive audio and video.

A malformed RTP packet can cause a vulnerable device to crash. These vulnerabilities are documented as the following Cisco Bug IDs:

- [CSCse68138 Issue in handling specific packets in VOIP RTP Lib](#) ([registered](#) customers only)
- [CSCse05642 I/O memory corruption crash on a router](#) ([registered](#) customers only)

Facsimile reception vulnerability

Reception of a large packet can cause a vulnerable device to crash. This vulnerability is documented as the following Cisco Bug ID:

- [CSCej20505 Router hangs with overly large packet](#) ([registered](#) customers only)

Vulnerability Scoring Details

Cisco is providing 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 1.0.

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

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

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

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>.

Note: To make this document more readable, individual CVSS scores for vulnerabilities are not shown. Instead, the vulnerabilities are grouped according to the score.

The following SIP-related vulnerabilities have identical CVSS scoring						
<ul style="list-style-type: none"> • CSCsi80749 (registered customers only) Calculate the environmental score ↗ • CSCsi80102 - CUCM Calculate the environmental score ↗ 						
CVSS Base Score - 10						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
Temporal Score - 8.3						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

The following SIP-related vulnerabilities have identical CVSS scoring						
<ul style="list-style-type: none"> • CSCsf11855 (registered customers only) Calculate the environmental score ↗ • CSCeb21064 (registered customers only) Calculate the environmental score ↗ • CSCse40276 (registered customers only) Calculate the environmental score ↗ • CSCse68355 (registered customers only) Calculate the environmental score ↗ • CSCsf30058 (registered customers only) Calculate the environmental score ↗ • CSCsb24007 (registered customers only) Calculate the environmental score ↗ • CSCsc60249 (registered customers only) Calculate the environmental score ↗ 						

CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

The following MGCP-related vulnerabilities have identical CVSS scoring

- [CSCsf08998](#) ([registered](#) customers only) Calculate the [environmental score](#) [↗](#)
- [CSCsd81407](#) ([registered](#) customers only) Calculate the [environmental score](#) [↗](#)

CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

The following H.323 signaling-related vulnerabilities have identical CVSS scoring

- [CSCsi60004](#) ([registered](#) customers only) Calculate the [environmental score](#) [↗](#)
- [CSCsg70474](#) ([registered](#) customers only) Calculate the [environmental score](#) [↗](#)

CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

The following RTP-related vulnerabilities have identical CVSS scoring

- [CSCse68138](#) ([registered](#) customers only) Calculate the [environmental score](#) [↗](#)
- [CSCse05642](#) ([registered](#) customers only) Calculate the [environmental score](#) [↗](#)

CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

CVSS score for the facsimile reception vulnerability						
<ul style="list-style-type: none"> • CSCej20505 (registered customers only) Calculate the environmental score ↗ 						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

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

☐ Impact

The impacts associated with individual vulnerabilities are listed according to vulnerability type. If not specifically called out, all vulnerabilities within the same category have an identical impact.

SIP-related vulnerabilities

Successful exploitation of the vulnerabilities listed as Cisco Bug ID [CSCsi80749](#) ([registered](#) customers only) and [CSCsi80102](#) ([registered](#) customers only) can potentially lead to remote code execution.

Successful exploitation of other SIP-related vulnerabilities listed in this advisory can cause the affected device to crash. Repeated exploitation could result in a sustained denial of service (DoS) attack.

MGCP-related vulnerabilities

Successful exploitation of the vulnerability listed as Cisco Bug ID [CSCsf08998](#) ([registered](#) customers only) can cause the affected device to become unresponsive. The device will not be able to establish any new connections, and a reboot is required to restore normal functionality.

Successful exploitation of the vulnerability listed as Cisco Bug ID [CSCsd81407](#) ([registered](#) customers only) can cause the affected device to crash. Repeated exploitation could result in a sustained denial of service (DoS) attack.

H.323 Signaling-related vulnerabilities

Successful exploitation of the vulnerabilities listed in this advisory can cause the affected device to crash. Repeated exploitation could result in a sustained denial of service (DoS) attack.

Real-time Transport Protocol-related vulnerabilities

Successful exploitation of the vulnerabilities listed in this advisory can cause the affected device to crash. Repeated exploitation could result in a sustained denial of service (DoS) attack.

Facsimile reception vulnerability

Successful exploitation of the vulnerability listed in this advisory can cause the affected device to crash. Repeated exploitation could result in a sustained denial of service (DoS) attack.

[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.

For further information about how Cisco IOS is built, numbered and maintained, please see the following URL: <http://www.cisco.com/warp/public/620/1.html>

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Release	First Fixed Release	Recommended Release
12.0	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)

12.0DA	Not Vulnerable	
12.0DB	Not Vulnerable	
12.0DC	Not Vulnerable	
12.0S	Not Vulnerable	
12.0SC	Not Vulnerable	
12.0SL	Not Vulnerable	
12.0SP	Not Vulnerable	
12.0ST	Not Vulnerable	
12.0SX	Not Vulnerable	
12.0SY	Not Vulnerable	
12.0SZ	Not Vulnerable	
12.0T	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0W	Not Vulnerable	
12.0WC	12.0(5)WC16	
12.0WT	Not Vulnerable	
12.0XA	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XB	Not Vulnerable	
12.0XC	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XD	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XE	Vulnerable; first fixed in 12.1(27b)E2	
12.0XF	Vulnerable; contact TAC	
12.0XG	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XH	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XI	Vulnerable; first fixed in 12.2(26c); available	12.2(46a)

	14-Aug-07	
12.0XJ	Not Vulnerable	
12.0XK	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XL	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XM	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XN	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XQ	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XR	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XS	Not Vulnerable	
12.0XV	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.0XW	Not Vulnerable	
Affected 12.1-Based Release	First Fixed Release	Recommended Release
12.1	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1AA	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1AX	Not Vulnerable	
12.1AY	Not Vulnerable	
12.1AZ	Not Vulnerable	
12.1CX	Not Vulnerable	
12.1DA	Not Vulnerable	
12.1DB	Not Vulnerable	

12.1DC	Not Vulnerable	
12.1E	12.1(27b)E2	
12.1EA	12.1(22)EA10	12.1(22)EA10a 12.1(22)EA10b; available 13-Sept-07
12.1EB	Not Vulnerable	
12.1EC	Vulnerable; first fixed in 12.2(4)BC1	12.3(17b)BC8 12.3(21a)BC3
12.1EO	Not Vulnerable	
12.1EU	Not Vulnerable	
12.1EV	Not Vulnerable	
12.1EW	Not Vulnerable	
12.1EX	Vulnerable; first fixed in 12.1(27b)E2	
12.1EY	Vulnerable; first fixed in 12.1(27b)E2	
12.1EZ	Vulnerable; first fixed in 12.1(27b)E2	
12.1GA	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1GB	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1T	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1XA	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1XB	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1XC	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1XD	Vulnerable; first fixed in 12.2(26c); available	12.2(46a)

	14-Aug-07	
12.1XE	Vulnerable; first fixed in 12.1(27b)E2	
12.1XF	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XG	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XH	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1XI	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
		12.3(23) 12.3(20a)

12.1XJ	Vulnerable; first fixed in 12.3(23)	12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XK	Not Vulnerable	
12.1XL	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XM	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07

12.1XN	Not Vulnerable	
12.1XO	Not Vulnerable	
12.1XP	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XQ	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XR	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a);

		available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XS	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1XT	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XU	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.3(23) 12.3(20a)

12.1XV	Vulnerable; first fixed in 12.3(23)	12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1XW	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1XX	Not Vulnerable	
12.1XY	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1XZ	Vulnerable; first fixed in 12.2(26c); available 14-Aug-07	12.2(46a)
12.1YA	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.3(23) 12.3(20a) 12.3(21b)

12.1YB	Vulnerable; first fixed in 12.3(23)	12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1YC	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1YD	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.3(23) 12.3(20a)

12.1YE	Vulnerable; first fixed in 12.3(23)	12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1YF	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1YG	Not Vulnerable	
12.1YH	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-

		07
12.1YI	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.1YJ	Not Vulnerable	
Affected 12.2-Based Release	First Fixed Release	Recommended Release
12.2	12.2(26c); available 14-Aug-07 12.2(27c); available 14-Aug-07 12.2(28d); available 14-Aug-07 12.2(29b); available 14-Aug-07 12.2(46a); available 15-Aug-07	12.2(46a)
12.2B	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f)

		12.4(16) 12.4(10c) 12.4(13d)
12.2BC	Not Vulnerable	
12.2BW	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2BY	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Vulnerable; contact TAC	
12.2DA	Not Vulnerable	

12.2DD	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2DX	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2EU	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	
12.2IXA	Vulnerable; first fixed in 12.2(18)IXD1	12.2(18)IXD1

12.2IXB	Vulnerable; first fixed in 12.2(18)IXD1	12.2(18)IXD1
12.2IXC	Vulnerable; first fixed in 12.2(18)IXD1	12.2(18)IXD1
12.2IXD	12.2(18)IXD1	12.2(18)IXD1
12.2IXE	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	12.2(15)MC1 12.2(15)MC2a 12.2(15)MC2i 12.2(8)MC1 12.2(8)MC2	12.2(15)MC2j
12.2S	12.2(14)S19 12.2(18)S13 12.2(20)S13 12.2(25)S13 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2SB	12.2(28)SB1 12.2(31)SB6	12.2(28)SB9; available 15-Aug-07 12.2(31)SB6
12.2SBC	Vulnerable; first fixed in 12.2(28)SB1	12.2(28)SB9; available 15-Aug-07 12.2(31)SB6
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	12.2(33)SRA5	12.2(33)SRA5
12.2SRB	12.2(33)SRB2; available 31-Aug-07	12.2(33)SRB2; available 31-Aug-07
12.2SU	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2SV	12.2(22)SV 12.2(23)SV 12.2(24)SV 12.2(25)SV 12.2(27)SV2 12.2(27)SV3 12.2(28)SV1 12.2(29)SV	12.2(29)SV4; available 14-Oct-07

	12.2(29a)SV	
12.2SVA	Not Vulnerable	
12.2SVC	Vulnerable; contact TAC	
12.2SW	12.2(20)SW 12.2(21)SW 12.2(21)SW1 12.2(25)SW10 12.2(25)SW11	12.2(25)SW11
12.2SX	Vulnerable; first fixed in 12.2(18)SXF10	
12.2SXA	Vulnerable; first fixed in 12.2(18)SXF10	
12.2SXB	Vulnerable; first fixed in 12.2(18)SXF10	12.2(18)SXF10
12.2SXD	Vulnerable; contact TAC	
12.2SXE	Vulnerable; first fixed in 12.2(18)SXF10	12.2(18)SXF10
12.2SXF	12.2(18)SXF10	12.2(18)SXF10
12.2SXH	Not Vulnerable	
12.2SY	Not Vulnerable	
12.2SZ	Vulnerable; first fixed in 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2T	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07

		12.3(17c); available 16-Aug-07
12.2TPC	12.2(8)TPC10c; available 17-Aug-07	12.2(8)TPC10c
12.2UZ	Not Vulnerable	
12.2VZ	Vulnerable; first fixed in 12.2(31)SB6	12.2(28)SB9; available 15-Aug-07 12.2(31)SB6
12.2XA	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XB	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.4(12c)

12.2XC	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2XD	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XE	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07

12.2XF	Not Vulnerable	
12.2XG	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XH	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XI	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07

		12.3(17c); available 16-Aug-07
12.2XJ	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XK	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XL	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a)

		12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XM	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XN	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.3(23) 12.3(20a) 12.3(21b) 12.3(22a)

12.2XQ	Vulnerable; first fixed in 12.3(23)	12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XR	Not Vulnerable	
12.2XS	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2XT	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.3(23) 12.3(20a)

12.2XU	Vulnerable; first fixed in 12.3(23)	<p>12.3(21b)</p> <p>12.3(22a)</p> <p>12.3(18a)</p> <p>12.3(19a); available 16-Aug-07</p> <p>12.3(17c); available 16-Aug-07</p>
12.2XV	Vulnerable; first fixed in 12.3(23)	<p>12.3(23)</p> <p>12.3(20a)</p> <p>12.3(21b)</p> <p>12.3(22a)</p> <p>12.3(18a)</p> <p>12.3(19a); available 16-Aug-07</p> <p>12.3(17c); available 16-Aug-07</p>
12.2XW	Vulnerable; first fixed in 12.3(23)	<p>12.3(23)</p> <p>12.3(20a)</p> <p>12.3(21b)</p> <p>12.3(22a)</p> <p>12.3(18a)</p> <p>12.3(19a); available 16-Aug-07</p> <p>12.3(17c); available 16-Aug-07</p>

12.2YA	12.2(4)YA12; available 17-Aug-07	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2YB	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2YC	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07

		12.3(17c); available 16-Aug-07
12.2YD	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YE	Vulnerable; first fixed in 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2YF	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
	Vulnerable; first fixed	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a)

12.2YG	in 12.3(23)	12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2YH	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2YJ	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.4(12c) 12.4(3h) 12.4(5c)

12.2YK	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YL	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YM	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
		12.4(12c) 12.4(3h) 12.4(5c)

12.2YN	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YO	Not Vulnerable	
12.2YP	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2YQ	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
		12.4(12c) 12.4(3h)

12.2YR	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YS	Vulnerable; contact TAC	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YT	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.4(12c)

12.2YU	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YV	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YW	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
		12.4(12c)

12.2YX	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YY	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YZ	Vulnerable; first fixed in 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2ZA	Not Vulnerable	
12.2ZB	12.2(8)ZB	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16)

		12.4(10c)
		12.4(13d)
12.2ZC	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
12.2ZF	Vulnerable; first fixed in 12.3(11)T12;	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07

	available 16-Aug-07	12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZG	Vulnerable; contact TAC	12.3(2)XA6 12.3(8)YG6; available 16-Aug-07
12.2ZH	12.2(13)ZH9; available 17-Aug-07	12.2(13)ZH9
12.2ZJ	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZL	Vulnerable, first fixed in 12.3(11)T12, available 16-Aug-07 for the Cisco 17xx; first fixed in 12.4(16) for the Cisco 3200; first fixed in 12.3(7) XR7, available 13-Aug-07 for the ICS7750	
		12.4(12c) 12.4(3h) 12.4(5c)

12.2ZP	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZR	Vulnerable; contact TAC	
12.2ZU	Vulnerable; first fixed in 12.2(33)SXH; available 31-Aug-07	12.2(33)SXH; available 31-Aug-07
12.2ZW	Vulnerable; contact TAC	
12.2ZY	12.2(18)ZY1	12.2(18)ZY2; available 14-Sep-07
Affected 12.3-Based Release	First Fixed Release	Recommended Release
12.3	12.3(17c); available 16-Aug-07 12.3(18a); available 16-Aug-07 12.3(19a); available 16-Aug-07 12.3(20a) 12.3(21b) 12.3(22a) 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); available 16-Aug-07 12.3(17c); available 16-Aug-07
		12.4(12c) 12.4(3h) 12.4(5c)

12.3B	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3BC	Not Vulnerable	
12.3BW	Not Vulnerable	
12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JK	Not Vulnerable	
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	
12.3T	Limited platform support is available 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3TPC	12.3(4)TPC11b; available 17-Aug-07	12.3(4)TPC11b; available 17-Aug-07
12.3VA	Not Vulnerable	
12.3XA	12.3(2)XA6	12.3(2)XA6
		12.4(12c)

12.3XB	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XC	12.3(2)XC5	12.3(2)XC5
12.3XD	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XE	12.3(2)XE5; available 17-Aug-07	12.3(2)XE5
12.3XF	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c)

		12.4(13d)
12.3XG	Vulnerable; contact TAC	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XH	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XI	12.3(7)XI1b 12.3(7)XI8a 12.3(7)XI2a	12.3(7)XI10a; available 21-Aug-07
12.3XJ	Vulnerable; first fixed in 12.3(14)YX9; available 13-Aug-07	12.3(14)YX9; available 13-Aug-07
		12.4(12c) 12.4(3h) 12.4(5c)

12.3XK	Vulnerable; first fixed in 12.3(11)T12; available 16-Aug-07	12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XQ	Vulnerable; first fixed in 12.4(16)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XR	12.3(7)XR7; available 17-Aug-07	12.3(7)XR7; available 17-Aug-07
12.3XS	Vulnerable; first fixed in 12.4(16)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
		12.4(11)T3

12.3XU	12.3(8)XU	12.4(9)T5; available 24-Aug-07 12.4(2)T6; available 20-Aug-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3XW	Vulnerable; first fixed in 12.3(14)YX9; available 13-Aug-07	12.3(14)YX9; available 13-Aug-07
12.3XY	Vulnerable; contact TAC	12.4(11)T3 12.4(9)T5; available 24-Aug-07 12.4(2)T6; available 20-Aug-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YA	Vulnerable; first fixed in 12.4(16)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16)

		12.4(10c) 12.4(13d) 12.3(8)YG6; available 16-Aug-07
12.3YD	Vulnerable; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; available 24-Aug-07 12.4(2)T6; available 20-Aug-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YF	Vulnerable; first fixed in 12.3(14)YX9; available 13-Aug-07	12.3(14)YX9; available 13-Aug-07
12.3YG	12.3(8)YG6; available 16-Aug-07	12.3(8)YG6; available 16-Aug-07
12.3YH	Vulnerable; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; available 24-Aug-07 12.4(2)T6; available 20-Aug-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(15)T1

12.3YI	Vulnerable; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; available 24-Aug-07 12.4(2)T6; available 20-Aug-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YJ	Not Vulnerable	
12.3YK	12.3(11)YK3; available 20-Aug-07	12.3(11)YK3; available 20-Aug-07
12.3YM	12.3(14)YM11; available 23-Aug-07	12.3(14)YM11; available 23-Aug-07
12.3YQ	Vulnerable; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; available 24-Aug-07 12.4(2)T6; available 20-Aug-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YS	Vulnerable; first fixed in 12.4(11)T3	12.3(11)YS2
		12.4(11)T3 12.4(9)T5;

12.3YT	Vulnerable; first fixed in 12.4(11)T3	available 24-Aug-07 12.4(2)T6; available 20-Aug-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YU	Vulnerable; first fixed in 12.4(2)XB6; available 16-Aug-07	12.4(2)XB6; available 16-Aug-07
12.3YX	12.3(14)YX9; available 13-Aug-07	12.3(14)YX9; available 13-Aug-07
12.3YZ	12.3(11)YZ2; available 17-Aug-07	12.3(11)YZ2; available 17-Aug-07
Affected 12.4-Based Release	First Fixed Release	Recommended Release
12.4	12.4(10c); available 20-Aug-07 12.4(12c) 12.4(13d) 12.4(16) 12.4(3h); available 20-Aug-07 12.4(5c); available 15-Aug-07 12.4(7f) 12.4(8d); available 3-Sep-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); available 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.4JA	Not Vulnerable	

12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	12.4(12)MR2; available 14-Aug-07	12.4(12)MR2
12.4SW	Not Vulnerable	
12.4T	12.4(11)T3 12.4(15)T1 12.4(2)T6; available 3- Sep-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(9)T5; available 24-Aug-07	12.4(11)T3 12.4(9)T5; available 24-Aug- 07 12.4(2)T6; available 20-Aug- 07 12.4(4)T8; available 28-Aug- 07 12.4(6)T8 12.4(15)T1
12.4XA	Vulnerable; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; available 24-Aug- 07 12.4(2)T6; available 20-Aug- 07 12.4(4)T8; available 28-Aug- 07 12.4(6)T8 12.4(15)T1
12.4XB	12.4(2)XB6; available 16-Aug-07	12.4(2)XB6; available 16-Aug- 07
12.4XC	12.4(4)XC7; available 17-Aug-07	12.4(4)XC7
	12.4(4)XD8; available	12.4(4)XD8;

12.4XD	13-Aug-07	available 30-Aug-07
12.4XE	12.4(6)XE3; available 17-Aug-07	12.4(6)XE3
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	12.4(11)XJ4	12.4(11)XJ4
12.4XK	Vulnerable; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; available 24-Aug-07 12.4(2)T6; available 20-Aug-07 12.4(4)T8; available 28-Aug-07 12.4(6)T8 12.4(15)T1
12.4XT	12.4(6)XT1; available 17-Aug-07	12.4(6)XT1
12.4XV	12.4(11)XV1; available 17-Aug-07	12.4(11)XV1
12.4XW	12.4(11)XW2 12.4(11)XW3; available 24-Aug-07	12.4(11)XW3; available 13-Aug-07

Fixed Software for Cisco Unified Communications Manager

CUCM Version	Fixed Release	Download Location
CUCM 3.3	Not affected	Software release 3.3 is not affected by CSCsi80102 (registered customers only)
CUCM 4.x	Not affected	None of 4.x software releases are affected by CSCsi80102 (registered customers only)

CUCM 5.0	Not Provided	Upgrade to CUCM 5.1(2b)
CUCM 5.1	5.1(2b)	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-51?psrtdcat20e2
CUCM 6.0	6.0(1a)	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-60

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

Workarounds

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 the application of anti-spoofing measures on the network edge. This action is required because all vulnerable voice protocols can use UDP as transport protocol.

None of the listed vulnerabilities can be mitigated on Cisco Unified Communications Manager. All mitigations must be done on adjacent devices.

Users are advised to disable affected protocols if not required for normal device operation. To prevent the router from processing SIP packets, the user must execute the following commands:

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

Note: When applying this workaround to devices that are processing MGCP or H.323 calls, the device will not allow SIP processing to stop while active calls are being processed. As a result, the workaround should be implemented during a maintenance period when active calls can be stopped.

Infrastructure Access Control Lists (iACL)

Although difficult to block traffic from transiting the network, it is possible to identify traffic that should not target infrastructure devices and block such traffic at the network border. Infrastructure ACLs are considered 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 ACL example shown below should be included as part of the deployed infrastructure access list that will protect all devices with IP addresses located within the infrastructure IP address range.

A sample access list for devices running Cisco IOS is below:

```
!-- Permit SIP, MGCP, H.323 and RTP services from trusted hosts destined
!-- to infrastructure addresses.

access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
```

```

    eq 5060
access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
    eq 5061
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
    eq 5060
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
    eq 5061
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
    eq 2427
access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
    eq 1720
access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
    eq 11720
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
    eq 2517
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
    range 16384 32767

```

```

!-- Deny SIP, MGCP, H.323 and RTP packets from all other sources destined
!-- to infrastructure addresses.

```

```

access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK eq 5060
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK eq 5061
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 5060
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 5061
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2427
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK eq 1720
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK eq 11720
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2517
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK
    range 16384 32767

```

```

!-- Permit all other traffic to transit the device.

```

```

access-list 150 permit ip any any
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. This white paper can be obtained at the following link:
<http://www.cisco.com/warp/public/707/iacl.html>.

Control Plane Policing

Control Plane Policing (CoPP) can be used to block untrusted SIP (TCP and UDP ports 5060 and 5061), MGCP (UDP port 2427), H.323 (TCP ports 1720 and 11720 and UDP port 2517), and RTP (UDP ports 16384 to 32767) access 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 may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks. CoPP protects the management and control planes by explicitly permitting only authorized traffic sent to infrastructure devices and in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to the network:

```
!-- Deny SIP, MGCP, H.323 and RTP traffic from trusted hosts to all
!-- IP addresses configured on all interfaces of the affected device
!-- so that it will be allowed by the CoPP feature.
```

```
access-list 111 deny tcp host 192.168.100.1 any eq 5060
access-list 111 deny tcp host 192.168.100.1 any eq 5061
access-list 111 deny udp host 192.168.100.1 any eq 5060
access-list 111 deny udp host 192.168.100.1 any eq 5061
access-list 111 deny udp host 192.168.100.1 any eq 2427
access-list 111 deny tcp host 192.168.100.1 any eq 1720
access-list 111 deny tcp host 192.168.100.1 any eq 11720
access-list 111 deny udp host 192.168.100.1 any eq 2517
access-list 111 deny udp host 192.168.100.1 any range 16384 32767
```

```
!-- Permit all other SIP, MGCP, H.323 and RTP traffic sent to all
!-- IP addresses configured on all interfaces of the affected device
!-- so that it will be policed and dropped by the CoPP feature.
```

```
access-list 111 permit tcp any any eq 5060
access-list 111 permit tcp any any eq 5061
access-list 111 permit udp any any eq 5060
access-list 111 permit udp any any eq 5061
access-list 111 permit udp any any eq 2427
access-list 111 permit tcp any any eq 1720
access-list 111 permit tcp any any eq 11720
access-list 111 permit udp any any eq 2517
access-list 111 permit udp any any range 16384 32767
```

```
!-- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!-- 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-voice-class
  match access-group 111
```

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

```
policy-map drop-voice-traffic
  class drop-voice-class
    drop
```

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

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

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in the exploit packets being discarded by the policy-map "drop" function. Meanwhile, packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

Please note that in the 12.2S and 12.0S Cisco IOS trains the policy-map syntax is different:

```
policy-map drop-voice-traffic
class drop-voice-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 at 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.

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: <http://www.cisco.com/warp/public/707/cisco-amb-20070808-IOS-voice.shtml>

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

▣ Obtaining Fixed Software

Cisco will make free software available to address these vulnerabilities for affected customers. This advisory will be updated as fixed software becomes available. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "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 agreement 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 who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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

Have your product serial number available and give the URL of this notice as evidence of your 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 special 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 vulnerabilities described in this advisory.

The following vulnerabilities were discovered during internal testing:

- CSCsi80749 Crash while processing malformed SIP packet
- CSCsi80102 CUCM - Crash while processing malformed SIP packet
- CSCeb21064 Crash while processing malformed SIP packet
- CSCse40276 Router crashed by malformed SIP message
- CSCse68355 Router crashed by malformed SIP packet
- CSCsf30058 Memory leak when processing malformed SIP message
- CSCsf08998 MGCP stop responding after receiving malformed packet
- CSCsd81407 Router crash on receiving abnormal MGCP messages
- CSCsg70474 IOS FW with h323 inspect crashes when malformed H.323 packets received
- CSCse68138 Issue in handling specific packets in VOIP RTP Lib

The following vulnerabilities were encountered in customer networks:

- CSCsf11855 Crash while processing malformed SIP packet
- CSCsb24007 Memory corruption and unexpected reload on receiving a SIP packet
- CSCsc60249 Crash while processing malformed SIP packet
- CSCsi60004 H323 Proxy Unregistration from Gatekeeper
- CSCse05642 I/O memory corruption crash on a router
- CSCej20505 Router hangs with overly large packet

[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-20070808-IOS-voice.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-teams@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 1.2	2007-August-20	Updated the SIP-related vulnerabilities for the Vulnerable Products section.
Revision 1.1	2007-August-08	Updated commands in the Infrastructure Access Control Lists (iACL) section.
Revision 1.0	2007-August-08	Initial public release.

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

☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

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

Help us help you.

☐
Please rate this document.

- ☐ Excellent
 Good
 Average
 Fair
 Poor

☐
This document solved my problem.

- ☐ Yes
 No
 Just browsing

☐
Suggestions for improvement:

(256 character limit)

☐

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

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

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