

# Cisco IOS Software H.323 Denial of Service Vulnerability

Advisory ID: cisco-sa-20090923-h323

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml>

## Revision 1.0

For Public Release 2009 September 23 1600 UTC (GMT)

---

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

---

## Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Summary

The H.323 implementation in Cisco IOS<sup>®</sup> Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml>.

**Note:** The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories.

Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

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

[http://www.cisco.com/web/about/security/intelligence/Cisco\\_ERP\\_sep09.html](http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html)

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

## ☐ Affected Products

### ☐ Vulnerable Products

Cisco devices that are running affected Cisco IOS Software versions that are configured to process H.323 messages are affected by this vulnerability. H.323 is not enabled by default.

To determine the Cisco IOS Software device is running H.323 services use the **show process cpu | include 323** command, as shown in the following example:

```
Router#show process cpu | include 323
 249      16000      3      5333  0.00%  0.00%  0.00%  0 CCH323_CT
 250         0      1         0  0.00%  0.00%  0.00%  0 CCH323_DNS
Router#
```

**Note:** Only H.323 listening port TCP 1720 is affected.

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

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

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih
```

*!--- output truncated*

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

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

*!--- output truncated*

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link: <http://www.cisco.com/web/about/security/intelligence/ios-ref.html>

## ☐ Products Confirmed Not Vulnerable

Cisco IOS XE and Cisco IOS XR Software are not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

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

## ☐ Details

H.323 is the ITU standard for real-time multimedia communications and conferencing over packet-based (IP) networks. A subset of the H.323 standard is H.225.0, a standard used for call signalling protocols and media stream packetization over IP networks.

The H.323 implementation in Cisco IOS Software contains a vulnerability. An attacker can exploit this vulnerability remotely by sending an H.323 crafted packet to the affected device that is running Cisco IOS Software. A TCP three-way handshake is needed to exploit this vulnerability.

This vulnerability is documented in Cisco bug ID [CSCsz38104](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-2866.

[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>.

**CSCsz38104 - Crafted H323 packets may cause device to reload**

Calculate the environmental score of [CSCsz38104](#)

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 - <b>6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## ▣ Impact

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

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

## ▣ Software Versions and Fixes

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

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

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for 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.

<b>Major Release</b>	<b>Availability of Repaired Releases</b>	
<b>Affected</b>		

12.0- Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases.		
Affected 12.1- Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases.		
Affected 12.2- Based Releases	First Fixed Release	Recommended Release
12.2	Not Vulnerable	
12.2B	Vulnerable; first fixed in <a href="#">12.4</a> Releases up to and including 12.2(4)B8 are not vulnerable.	12.4(25b) 12.4(23b)
12.2BC	Not Vulnerable	
12.2BW	Not Vulnerable	
12.2BX	Vulnerable; first fixed in <a href="#">12.4</a> Releases up to and including 12.2(15)BX are not vulnerable.	12.4(25b) 12.4(23b)
12.2BY	Not Vulnerable	

12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Vulnerable; migrate to 12.2SB	12.2(33)SB7
12.2DA	Not Vulnerable	
12.2DD	Not Vulnerable	
12.2DX	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	
12.2EX	Not Vulnerable	
12.2EY	Not Vulnerable	
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	

12.2FY	Not Vulnerable	
12.2FZ	Not Vulnerable	
12.2IRA	Not Vulnerable	
12.2IRB	Not Vulnerable	
12.2IRC	Not Vulnerable	
12.2IXA	Not Vulnerable	
12.2IXB	Not Vulnerable	
12.2IXC	Not Vulnerable	
12.2IXD	Not Vulnerable	
12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2IXG	Not Vulnerable	
12.2IXH		

	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Releases up to and including 12.2(15)MC1 are not vulnerable. Releases 12.2(15)MC2b and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.2S	Not Vulnerable	
12.2SB	Not Vulnerable	
12.2SBC	Not Vulnerable	
12.2SCA	Not Vulnerable	
12.2SCB	Not Vulnerable	
12.2SE	Not Vulnerable	
12.2SEA	Not Vulnerable	

12.2SEB	Not Vulnerable	
12.2SEC	Not Vulnerable	
12.2SED	Not Vulnerable	
12.2SEE	Not Vulnerable	
12.2SEF	Not Vulnerable	
12.2SEG	Not Vulnerable	
12.2SG	Not Vulnerable	
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SQ	Not Vulnerable	
12.2SRA	Not Vulnerable	

12.2SRB	Not Vulnerable	
12.2SRC	Not Vulnerable	
12.2SRD	Not Vulnerable	
12.2STE	Not Vulnerable	
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SVE	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA		

	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Not Vulnerable	
12.2SXE	Not Vulnerable	
12.2SXF	Not Vulnerable	
12.2SXH	Not Vulnerable	
12.2SXI	Not Vulnerable	
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Vulnerable; first fixed in <a href="#">12.4</a> Releases up to and including 12.2(8)T10 are not vulnerable.	12.4(25b) 12.4(23b)
12.2TPC	Not Vulnerable	
12.2XA	Not Vulnerable	
12.2XB		

	Not Vulnerable	
12.2XC	Not Vulnerable	
12.2XD	Not Vulnerable	
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	
12.2XG	Not Vulnerable	
12.2XH	Not Vulnerable	
12.2XI	Not Vulnerable	
12.2XJ	Not Vulnerable	
12.2XK	Not Vulnerable	
12.2XL	Not Vulnerable	
12.2XM	Not Vulnerable	
12.2XNA	Not Vulnerable	

12.2XNB	Not Vulnerable	
12.2XNC	Not Vulnerable	
12.2XND	Not Vulnerable	
12.2XO	Not Vulnerable	
12.2XQ	Not Vulnerable	
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Not Vulnerable	
12.2XU	Not Vulnerable	
12.2XV	Not Vulnerable	
12.2XW	Not Vulnerable	
12.2YA	Not Vulnerable	
12.2YB	Not Vulnerable	

12.2YC	Not Vulnerable	
12.2YD	Not Vulnerable	
12.2YE	Not Vulnerable	
12.2YF	Not Vulnerable	
12.2YG	Not Vulnerable	
12.2YH	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2YJ	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2YK	Not Vulnerable	
12.2YL	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2YM	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.2YN	Vulnerable; Contact your support organization per the instructions in <a href="#">Ob</a>	

	<a href="#">taining Fixed Software</a> section of this advisory	
12.2YO	Not Vulnerable	
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	
12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2YU	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2YV	Releases prior to 12.2(11)YV1 are vulnerable, release 12.2(11)YV1 and later are not vulnerable	
12.2YW	Not Vulnerable	
12.2YX	Not Vulnerable	
12.2YY	Not Vulnerable	

12.2YZ	Not Vulnerable	
12.2ZA	Not Vulnerable	
12.2ZB	Not Vulnerable	
12.2ZC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2ZD	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2ZE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.2ZF	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.2ZG	Not Vulnerable	
12.2ZH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.2ZJ	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	

12.2ZL	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2ZP	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.2ZU	Not Vulnerable	
12.2ZX	Not Vulnerable	
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.3	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3B	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3BC	Not Vulnerable	
12.3BW	Not Vulnerable	

12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	
12.3JK	Releases up to and including 12.3(2)JK3 are not vulnerable.	12.4(25b)
	Releases 12.3(8)JK1 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(23b)
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	
12.3T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3TPC	Releases up to and including 12.3(4)TPC11a are not vulnerable.	
12.3VA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2;

		Available on 23-OCT-2009
12.3XA	Releases prior to 12.3(2)XA7 are vulnerable, release 12.3(2)XA7 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XB	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.3XC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XF	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.3XG	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XI	Note: Releases prior to 12.3(7)XI11 are vulnerable, release 12.3(7)XI11 and later are not vulnerable;	12.2(33)SB7 12.2(31)SB16
12.3XJ	Vulnerable; migrate to any release in 12.4XN	12.4(15)T10

12.3XK	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XQ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XR	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XS	Not Vulnerable	
12.3XU	Vulnerable; first fixed in <a href="#">12.4T</a> Releases up to and including 12.3(8)XU1 are not vulnerable.	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3XW	Vulnerable; migrate to any release in 12.4XR	12.4(15)XR7 12.4(22)XR
12.3XX	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XY	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b) 12.4(23b)
12.3XZ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(25b)

		12.4(23b)
12.3YA	Not Vulnerable	
12.3YD	Not Vulnerable	
12.3YF	Vulnerable; migrate to any release in 12.4XR	12.4(15)XR7 12.4(22)XR
12.3YG	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YH	Not Vulnerable	
12.3YI	Not Vulnerable	
12.3YJ	Not Vulnerable	
12.3YK	Releases prior to 12.3(11)YK3 are vulnerable, release 12.3(11)YK3 and later are not vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
		12.4(15)T10

12.3YM	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YQ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YS	Vulnerable; first fixed in <a href="#">12.4T</a> Releases up to and including 12.3(11)YS1 are not vulnerable.	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YU	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
		12.4(15)XR7

12.3YX	Vulnerable; migrate to <a href="#">12.4XR</a>	12.4(22)XR
12.3YZ	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.3ZA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
<b>Affected 12.4- Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	12.4(25b) 12.4(23b)	12.4(25b) 12.4(23b)
12.4GC	Not Vulnerable	
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JDC	Not Vulnerable	
12.4JDD	Not Vulnerable	

12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MDA	Not Vulnerable	
12.4MR	Releases prior to 12.4(19)MR3 are vulnerable, release 12.4(19)MR3 and later are not vulnerable	
12.4SW	Not Vulnerable	
12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T2 12.4(24)T1	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
		12.4(15)T10 12.4(20)T4

12.4XA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XB	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XC	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XD	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XE	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XF	Not Vulnerable	

12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XK	Not Vulnerable	
12.4XL	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.4XM	Vulnerable; first fixed in <a href="#">12.4T</a> Releases up to and including 12.4(15)XM are not vulnerable.	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XN	Not Vulnerable	
12.4XP	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.4XQ	Not Vulnerable	

12.4XR	Not Vulnerable	
12.4XT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XV	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.4XW	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XY	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XZ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.4YA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YB	12.4(22)YB4	12.4(22)YB4
12.4YD	Not Vulnerable	
12.4YE	Not Vulnerable	

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

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

## ☐ Workarounds

There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the Cisco IOS device does not need to run H.323 for VoIP services. Affected devices that must run H.323 are vulnerable, and there are not any specific configurations that can be used to protect them. Applying access lists on interfaces that should not accept H.323 traffic and putting firewalls in strategic locations may greatly reduce exposure until an upgrade can be performed.

Cisco provides Solution Reference Network Design (SRND) guides to help design and deploy networking solutions, which can be found at <http://www.cisco.com/go/srnd> Voice Security best practices are covered in the Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/srnd/6x/security.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/security.html).

Below is an example of an access list to block H.323 management traffic from anywhere but a permitted network. In this example, the permitted network is 172.16.0.0/16.

```
!--- Permit access from any IP address in the 172.16.0.0/16
!--- network to anywhere on port 1720.

access-list 101 permit tcp 172.16.0.0 0.0.255.255 any eq 1720

!--- Permit access from anywhere to a host in the
!--- 172.16.0.0/26 network on port 1720.

access-list 101 permit tcp any 172.16.0.0 0.0.255.255 eq 1720
```

```
!--- Deny all traffic from port 1720.

access-list 101 deny tcp any eq 1720 any

!--- Deny all traffic to port 1720.

access-list 101 deny tcp any any eq 1720

!--- Permit all other traffic.

access-list 101 permit ip any any
```

Alternatively, you can use the **call service stop forced** command under the **voice service voip** mode, as shown in the following example:

```
voice service voip
  h323
    call service stop forced
```

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Cisco Unified Communications Manager and Cisco IOS Software", which is available at the following location: <http://www.cisco.com/warp/public/707/cisco-amb-20090923-voice.shtml>.

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

## ☐ **Obtaining Fixed Software**

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

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at [http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\\_.htm](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.htm), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto:security-alert@cisco.com) for software upgrades.

### ☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

### ☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and

releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

## ☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

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

## ☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was found during internal testing.

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

## ☐ **Status of this Notice: FINAL**

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

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

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

## ☐ **Distribution**

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

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml>

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

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

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

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

## ☐ Revision History

Revision 1.0	2009-September-23	Initial public release
--------------	-------------------	------------------------

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

## ☐ Cisco Security Procedures

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

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

---

**Help us help you.**

**Please rate this document.**

- Excellent
- Good
- Average
- Fair
- Poor

**This document solved my problem.**

Yes

No

Just browsing

**Suggestions for improvement:**

(256 character limit)

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

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

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