

Cisco Security Advisory: Vulnerabilities in H.323 Message Processing

Revision 1.4 - INTERIM

Last Updated 2004 October 08 UTC 1330

For Public Release 2004 January 13 UTC 1200

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

Contents

[Summary](#)

[Affected Products](#)

[Unaffected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Obtaining Fixed Software](#)

[Workarounds](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: INTERIM](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Multiple Cisco products contain vulnerabilities in the processing of H.323 messages, which are typically used in Voice over Internet Protocol (VoIP) or multimedia applications. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS® Software Release 11.3T. Release 11.3T, and all later Cisco IOS releases may be affected if the software includes support for voice/multimedia applications. Vulnerable devices include those that contain software support for H.323 as network elements as well as those configured for IOS Network Address Translation (NAT) and those configured for IOS Firewall (also known as Context-Based Access Control [CBAC]).

Other Cisco voice products that do not run Cisco IOS may also be affected.

These vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml>.

Affected Products

All Cisco products that run Cisco IOS software and support H.323 packet processing are affected. This may include devices configured for Session Initiation Protocol (SIP) or Media Gateway Control Protocol (MGCP), since support for these protocols can enable support for H.323. Cisco IOS images with the "PLUS" feature set may be vulnerable regardless of their configuration because of a bug that enables H.323 by default and does not allow the protocol to be turned off.

Other affected products that do not run Cisco IOS software include:

- Cisco CallManager versions 3.0 through 3.3
- Cisco Conference Connection (CCC)
- Cisco Internet Service Node (ISN)
- Cisco BTS 10200 Softswitch
- Cisco 7905 IP Phone H.323 Software Version 1.00
- Cisco ATA 18x series products running H.323/SIP loads with versions earlier than 2.16.1

Note: Cisco ATA 18x series products are only vulnerable when configured for H.323. They are not vulnerable when configured for SIP.

To determine the software running on a Cisco 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 IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco product running Cisco IOS Software Release 12.0(3) with an installed image name of C2500-IS-L. The release train label is 12.0.

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

The following example shows a product running Cisco IOS Software Release 12.0(2a)T1 with an image name of C2600-JS-MZ.

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

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

If you are running Cisco IOS versions 10.x, 11.1, 11.2 or earlier, you are not affected.

Cisco IOS Processing of H.323 Traffic

There are three areas where IOS can be vulnerable to malformed H.323 packets. Please read the following sections to determine if your router is affected. If you need to open a TAC case, please capture the output of the suggested identification steps to speed your case resolution.

Note: If you choose to block H.323 traffic using an access list to prevent H.323 traffic from entering the router, you will have protected your device from the vulnerability described in this Advisory and the details listed below will not apply to you. Please see the [Workarounds](#) section for more details on how to do this. Cisco recommends that customers upgrade to an appropriate IOS image at their earliest convenience.

To determine if your Cisco IOS device is processing H.323 traffic and is possibly vulnerable, it is necessary to understand the three different ways that Cisco IOS software processes H.323 traffic.

1. H.323 Endpoints

This includes H.323 Gateway, H.323 Gatekeeper, and H.323 Gatekeeper with Proxy, as well as releases that may run the H.323 process by default without being configured. Please continue with the following steps to determine if your device is affected.

From the enable prompt, run the **show process cpu** command and look for a process called CCH323_CT. In later versions of Cisco IOS software, you can execute the **show process cpu | include CCH323**.

```
Router# show process cpu | include CCH323
112 Mwe 60F3E5E0          295112      239401      123220072/24000  0 CCH323_CT
```

Note: Only images with a "PLUS" feature set (such as IP PLUS, ENTERPRISE PLUS) support voice and will have the CCH323_CT process running. In 12.0, the "PLUS" feature set has the CCH323_CT process running by default on the 2600 and 3600 platforms. Starting in 12.1, the process will run by default if you have a voice card or dsp card inserted.

- If you see the a process called CCH323_CT, your router is affected. Please consult the IOS table to determine which version is appropriate for your device. If you cannot immediately upgrade, the following workarounds may work for you
 - If you *are not* using H.323 within your network, an inbound access list to block TCP port 1720 will protect your router, but it is recommended that you upgrade as soon as is feasible.
 - If you *are* using H.323, then you can configure an access list to restrict TCP port 1720 traffic to known, trusted IP addresses. Again, upgrading as soon as is feasible is recommended.
- If you do *not* see the CCH323_CT process, you may still be vulnerable. Some configurations of H.323 Gatekeeper are vulnerable. Affected configurations are those gatekeepers configured for H.323 Proxy. To check to see if you are configured as a gatekeeper, check your configuration for the line "proxy h323" in the global configuration. If you have "proxy h323" configured, then you are vulnerable.
 - If you *are not* using GK proxy functionality, you can disable proxy functionality by doing the following configuration.

Note: This will drop all calls being managed by the gatekeeper. Perform this only when you can safely stop gatekeeper functionality.

```
Router(config)#no proxy h323
Router(config)#gatekeeper
Router(config-gk)#shutdown
Router(config-gk)#no shutdown
```

- If you *are* using H.323 proxy, your options are to either configure an access list to restrict TCP port 1720 traffic to known, trusted IP addresses, or to upgrade your IOS version.

2. IOS Firewall (Context-Based Access Control)

If your IOS device is configured to use IOS Firewall (IOS FW, or Context-Based Access Control [CBAC]), check to see if IOS FW is running on the device by issuing the **show ip inspect all** command. Look for the following lines indicating that IOS FW is applied to an interface. In this case, inspection rule "<NAME>" is applied inbound to interface FastEthernet0/0.

```
Interface Configuration
Interface FastEthernet0/0
Inbound inspection rule is <NAME>
tcp alert is on audit-trail is off timeout 3600
h323 alert is on audit-trail is off timeout 3600
Outgoing inspection rule is not set
```

- To turn off inbound IOS FW (CBAC) on interface FastEthernet0/0, enter the following commands in interface configuration mode.

```
Router#config t
Router(config)#Interface FastEthernet 0/0
Router(config-if)#no ip inspect <NAME> in
```

- If outbound IOS FW (CBAC) is configured on FastEthernet0/0, enter the following commands in interface configuration mode.

```
Router#config t
Router(config)#Interface FastEthernet 0/0
Router(config-if)#no ip inspect <NAME> out
```

- To turn off the IOS FW (CBAC) processing of H.323 messages only while leaving other IOS FW behavior unaffected, enter the following command in global configuration mode.

```
Router(config)#no ip inspect name <NAME> h323
```

Cisco recommends that you upgrade your IOS as soon as possible.

3. IOS Network Address Translation (NAT)

If you have configured NAT rules and have NAT activated on any interface, check to see if NAT is configured and activated on the device by issuing the **show ip nat statistics** command.

```
Router#show ip nat statistics
```

```
Total active translations: 3 (3 static, 0 dynamic; 0 extended)
Outside interfaces
Inside interfaces
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
```

- If there is no output or the output doesn't list any inside or outside interfaces (as in the example above), then the IOS device is not doing NAT and you are not vulnerable because of NAT.
- If the output *does* list any inside or outside interfaces, then you may be vulnerable because of NAT. An example is shown below.

```
Total active translations: 3 (3 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial3/0
Inside interfaces:
  Serial11/0
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
```

- You are *not* vulnerable because of NAT if your configuration only contains Port Address Translation (PAT) statements and your PAT statements *do not* explicitly specify TCP port 1720 in your PAT translations.
 - To see if you are doing only PAT, check to see if your IOS NAT configuration contains any of the following NAT rules without the **overload**, **route-map**, or **extendable** keywords.

```
ip nat outside source ...
ip nat inside destination ...
ip nat inside source ...
```

If you see any of the above lines without the **overload**, **route-map**, or **extendable** keywords, then you are vulnerable.

- To see if you are doing a static PAT for H.323 (TCP port 1720), look for any lines with the following pattern.

```
ip nat (inside|outside) source static tcp
ip-addr (port|1720) ip-addr (1720|port)
```

The following examples would be vulnerable.

```
ip nat inside source static tcp 10.1.0.1 1720 10.2.0.1 5834
ip nat outside source static tcp 10.15.12.1 6884 10.6.7.1 1720
```

```
ip nat inside source static tcp 10.1.0.17 1720 10.33.14.1 1720
```

The following examples would *not* be vulnerable.

```
ip nat inside source static tcp 10.1.0.17 53 10.33.14.1 53
```

```
ip nat outside source static udp 10.1.14.75 1720 10.131.1.1 6888
```

If any of your configuration lines are vulnerable, please consult the [Workarounds](#) section.

To determine if a particular Cisco IOS release is vulnerable, consult the list below in the [Software Versions and Fixes](#) section to determine if the product is running an affected version of software.

Unaffected Products

The following list of Cisco products is provided specifically to list those products that customers may also be concerned about in regards to these vulnerabilities. The products below are not affected either because they are not vulnerable or because they do not support H.323 processing. Any other Cisco products that have not been identified as vulnerable or have been omitted from the list below should be considered as not vulnerable, as no other Cisco products are known to be affected by these vulnerabilities.

- Cisco IP Phone models 7960, 7940, 7912, 7910, 7902, 30VIP, and 12SP+
- Cisco uOne (All Versions)
- VG248 Analog Phone Gateway
- Cisco Unity Server
- Catalyst 6000 WS-X6608 Voice Services Module and WS-X6624 FXS Analog Station Interface Module
- PGW2200, SC2200, VSC3000 and H.323 Signalling Interface (HSI)
- Cisco IP/VC 3500 Series
- IP/TV series
- Catalyst 19xx, 28xx, 290x, 292x, 2948g, 3000, 3200, 3900, 4000, 4912g, and 5000 series switches
- Catalyst 2900XL, 2900XL-LRE, 2940, 2950, 2950-LRE, 2955, 2970, 3500XL, 3550, and 3750 series switches
- Cache Engine series
- Content Engine series
- SN5400 series storage routers
- VPN 3000 and VPN 5000 series VPN concentrators
- Voice Interworking Service Module (VISM)
- VCO/4K
- Cisco Secure Intrusion Detection System (NetRanger) appliance and IDS Module
- BR340, WGB340, AP340, AP350, and BR350 Cisco/Aironet wireless products
- Cisco Aironet 1100 series, 1200 series, and 1400 series wireless products
- Cisco PIX Firewall
- Cisco Catalyst 6500 Series Firewall Services Module
- Cisco 6xx series DSL modems running CBOS
- Cisco 7xx series routers
- Cisco 12000 series routers
- Cisco 10000 series routers
- 61xx and 62xx series DSLAMs
- Cisco CSS11xxx series (including SSL Accelerator)
- LocalDirector
- BPX, IGX, MGX WAN switches, and the Service Expansion Shelf

- Cisco Intelligent Contact Management (ICM)
- Cisco ONS 15xxx platforms

Details

H.323 is the International Telecommunications Union (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.225.0 standard defines message formats for call setup, call control, and communications using Abstract Syntax Notation One (ASN.1). ITU Standard Q.931, which was developed for call signalling purposes in ISDN networks, is also used as the standard for the call setup messages within H.225.0.

The University of Oulu Secure Programming Group (OUSPG) has created a test suite for H.323, more specifically the H.225.0 and Q.931 messages, to help support proactive discovery and resolution of vulnerabilities in the processing of H.323 messages. The test suite is generally used to analyze a protocol and produce messages that probe various design limits within an implementation of a protocol. Test packets containing overly long or exceptional elements in various fields of the H.323 Protocol Data Units (PDUs) can be programmatically generated and then transmitted to a network device under test. The PROTOS test suite for H.323, as distributed, contains approximately 4500 individual test cases.

The vulnerabilities discovered in the affected products can be easily and repeatedly demonstrated with the use of the OUSPG PROTOS Test Suite for H.323. The largest group of vulnerabilities described in this advisory result from insufficient checking of H.225.0 messages as they are received and processed by an affected system. Malformed H.225.0 messages received by affected systems can cause various parsing and processing functions to fail, which may result in a system crash and reload (or reboot) in most circumstances.

Typically, H.323 network elements implement call signalling over both UDP and TCP transports on port 1720. The H.323 test suite from OUSPG only tests the TCP implementation on port 1720 by default.

Cisco IOS

Cisco IOS Software Release	Description of Vulnerability
11.1, 11.2, 11.3, 12.3	Not vulnerable
11.3T, 12.0, 12.0S, 12.0T, 12.1, 12.1T, 12.1E, 12.2, 12.2S, 12.2T	Vulnerabilities exist in the processing of H.323 Network Element traffic. This includes H.323 Gateway, H323 Gatekeeper, and H.323 Gatekeeper with Proxy.
12.1, 12.1E, 12.2, 12.2T, 12.2S, 12.3T	Vulnerabilities exist in the processing of H.323 IOS NAT traffic.
12.0, 12.1, 12.1E, 12.2, 12.2T, 12.2S	Vulnerabilities exist in the processing of H.323 IOS Firewall (CBAC) traffic.

The vulnerabilities in Cisco IOS for devices acting as H.323 dial-peer endpoints are documented in the following Bug IDs: [CSCdt09262](#) ([registered](#) customers only), [CSCdt54401](#) ([registered](#) customers only), [CSCdw14262](#) ([registered](#) customers only), [CSCdx76632](#) ([registered](#) customers only), [CSCdx77253](#) ([registered](#) customers only), [CSCea19885](#) ([registered](#) customers only), [CSCea32240](#) ([registered](#) customers only), [CSCea36231](#) ([registered](#) customers only), [CSCea33065](#) ([registered](#) customers only), [CSCea42826](#) ([registered](#) customers only), [CSCea42527](#) ([registered](#) customers only), [CSCea44227](#) ([registered](#) customers only), [CSCea44309](#) ([registered](#) customers only), [CSCea46342](#) ([registered](#) customers only), and [CSCec79541](#) ([registered](#) customers only).

For those Cisco IOS devices acting as a H.323 gatekeeper with proxy configured, the vulnerabilities are documented in the following Bug IDs: [CSCea51076](#) ([registered](#) customers only) , [CSCea51030](#) ([registered](#) customers only) , and [CSCea54851](#) ([registered](#) customers only) .

Cisco IOS devices performing NAT translations on H.323 v3/4 traffic may be vulnerable. Releases based off 12.2T must be running a version of IOS that is based off 12.2(11)T or later and must have the hidden command **ip nat service h323all** enabled. The default condition for this command is disabled. In releases based off 12.1 and 12.1E, the device is only vulnerable to packets sent from the outside interface to the inside interface. This means that networks are only vulnerable if they have static translations configured and accept connections to port 1720. A dynamic translation can occur on port 1720, but the attack traffic would then have to return from the destination address of the original flow and must traverse the router while the translation is still active. Methods to reduce exposure for dynamic translations are listed in the [Workarounds](#) section.

The vulnerabilities in Cisco IOS for devices doing NAT on H.323 packets starting in IOS 12.1 are documented in the following Bug IDs: [CSCdr48143](#) ([registered](#) customers only) , [CSCdx40184](#) ([registered](#) customers only) , [CSCea27536](#) ([registered](#) customers only) , [CSCec76694](#) ([registered](#) customers only) , and [CSCed28873](#) ([registered](#) customers only) .

The vulnerabilities in Cisco IOS for devices running IOS Firewall Feature Set doing deep packet inspection of H.323 packets in IOS starting in 12.1 are documented in the following Bug IDs: [CSCec76776](#) ([registered](#) customers only) and [CSCec87533](#) ([registered](#) customers only) .

Cisco CallManager

The vulnerabilities in Cisco CallManager are documented in Bug IDs [CSCdx82831](#) ([registered](#) customers only) , [CSCea46545](#) ([registered](#) customers only) , and [CSCea55518](#) ([registered](#) customers only) .

In order for a Cisco CallManager running 3.1 or 3.2 to be vulnerable, the IP address of the originating device must be configured as a H.323 gateway, H.323 client, or intercluster trunk on the CallManager, or "Allow Anonymous Calls" must be enabled in the gatekeeper section of the CallManager configuration. If a CallManager receives H.323 messages from a device that is not configured as an H.225.0 device, the TCP session will be closed before the H.225.0 message is processed. If "Allow Anonymous Calls" is enabled in the gatekeeper configuration, the CallManager server is vulnerable since it will try to parse the H.225.0 message from any originating source.

In CallManager 3.3, the server is vulnerable and will try to parse H.225.0 messages received from any originating source, but the CallManager may be listening on a port other than TCP 1720. Since the port number for anonymous calls is something other than TCP 1720, a potential attacker would need to determine which random port the CallManager H.323 gateway is listening on in order to carry out a successful attack.

Cisco Conference Connection

All versions of Cisco Conference Connection (CCC) are affected. There are currently no software fixes planned for Cisco Conference Connection (CCC). Customers running CCC should implement a workaround to limit H.323 traffic from trusted hosts only. A workaround for this may be found in the [Workarounds](#) section.

Cisco Internet Service Node

All versions of Internet Service Node (ISN) are affected. There are currently no software fixes planned for Cisco Internet Service Node (ISN). Customers running ISN should implement a workaround to limit H.323 traffic from trusted hosts only. A workaround for this may be found in the [Workarounds](#) section.

Cisco 7905 Series IP Phone

The vulnerabilities in the Cisco 7905 IP Phone are documented in Bug ID [CSCec77152](#) ([registered](#) customers only) .

Cisco ATA18x Series Analog Telephony Devices

The vulnerabilities in the Cisco ATA18x devices are documented in Bug IDs [CSCea46231](#) ([registered](#) customers only) ,

[CSCea48726](#) ([registered](#) customers only) and [CSCef42352](#) ([registered](#) customers only) .

Cisco BTS 10200 Softswitch

The vulnerabilities in the Cisco BTS 10200 Softswitch are documented in BugID [CSCea48755](#) ([registered](#) customers only) .

Impact

The vulnerabilities may be exploited to produce a denial of service (DoS) attack. When the vulnerabilities are exploited, they may cause an affected product to crash and reload. In the case of the Cisco CallManager, ISN, and CCC, exploitation will result in a crash or a hang indicated by processor utilization of 100%. When the CPU utilization is at 100% on server-based platforms, call processing services degrade severely, calls may drop, and no new calls can be established. A reboot of the device is required to return it to normal service.

Software Versions and Fixes

Cisco IOS Software

Each row of the table describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix and the anticipated date of availability for each are listed in the Rebuild, Interim, and Maintenance columns. In some cases, no rebuild of a particular release is planned; this is marked with the label "Not scheduled." A device running any release in the given train that is earlier than the release in a specific column (less than the earliest fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the earliest fixed release label).

When selecting a release, keep in mind the following definitions.

- **Maintenance**
Most heavily tested and highly recommended release of any label in a given row of the table.
- **Rebuild**
Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific vulnerability. Although it receives less testing, it contains only the minimal changes necessary to effect the repair. Cisco has made available several rebuilds of mainline trains to address this vulnerability, but strongly recommends running only the latest maintenance release on mainline trains.
- **Interim**
Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco Technical Assistance Center (TAC).

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 TAC for assistance, as shown in the section following this table.

Note: For the purposes of the table below, the identifier "Element" covers the fixes for IOS devices running as H.323 endpoints and as gatekeepers with proxy configured.

Train	Vulnerable Configuration	Availability of Fixed Releases		
10.x-based Releases		Not Vulnerable		
11.x-based Releases		Rebuild	Interim	Maintenance
11.0		Not Vulnerable		

11.1		Not Vulnerable		
11.1AA		Not Vulnerable		
11.1CA		Not Vulnerable		
11.1CC		Not Vulnerable		
11.2		Not Vulnerable		
11.2P		Not Vulnerable		
11.2SA		Not Vulnerable		
11.3		Not Vulnerable		
11.3T		Introduced H.323 feature in 11.3(3)T Vulnerable No Software Fixes Scheduled Migrate to 12.0		
12.0-based Releases		Rebuild	Interim	Maintenance
12.0	Element			12.0(27)
	NAT	Not Vulnerable		
	IPFW	12.0(28)		
12.0D		Not Vulnerable		
12.0DA		Not Vulnerable		
12.0DC		Not Vulnerable		
12.0S	Element	2600/3600 Platforms ONLY 12.0(25)S1, 12.0(24)S2, 12.0(23)S3		2600/3600 Platforms ONLY 12.0(26)S
	NAT	Not Vulnerable		
	IPFW	Not Vulnerable		
12.0SC		Not Vulnerable		
12.0SL		Not Vulnerable		
12.0SP		Not Vulnerable		
12.0ST		No fixes planned, only 2600/3600 platforms vulnerable		
12.0SX		Not Vulnerable		
12.0SY		Not Vulnerable		
12.0SZ		Not Vulnerable		
12.0T		Vulnerable. No fixes planned.		
12.0W5		Not Vulnerable		

12.0WC		Not Vulnerable		
12.0WT		Not Vulnerable		
12.0XC		Vulnerable. Migrate to 12.1(22)		
12.0XD		Vulnerable. Migrate to 12.1(22)		
12.0XG		Vulnerable. Migrate to 12.1(22)		
12.0XH		Vulnerable. Migrate to 12.1(22)		
12.0XI		Vulnerable. Migrate to 12.1(22)		
12.0XJ		Vulnerable. Migrate to 12.1(22)		
12.0XK		Vulnerable. Migrate to 12.2(19)b		
12.0XL		Vulnerable. Migrate to 12.1(22)		
12.0XN		Vulnerable. Migrate to 12.1(22)		
12.0XQ		Vulnerable. Migrate to 12.1(22)		
12.0XR		Vulnerable. Migrate to 12.2(19)b		
12.0XT		Vulnerable. No migration path		
12.1-based Releases		Rebuild	Interim	Maintenance
12.1	Element			12.1(22)
	NAT			12.1(22)
	IPFW			12.1(22)
12.1AA		Vulnerable. Migrate to 12.2(19)b		
12.1AX		Not Vulnerable		
12.1AY		Not Vulnerable		
12.1DA		Not Vulnerable		
12.1DB		Not Vulnerable		
12.1DC		Not Vulnerable		
12.1E	Element	12.1(20)E2		
	NAT	12.1(13)E13, 12.1(20)E2 12.1(8b)E18, 12.1(11b)E14, 12.1(14)E10, 12.1(19)E6 - available by 16-Jan-2004		

	IPFW	12.1(8b)E16, 12.1(11b)E14, 12.1(13)E12, 12.1(14)E9, 12.1(19)E6, 12.1(20)E2		
12.1EA		Not Vulnerable		
12.1EB		Not Vulnerable		
12.1EC		Vulnerable No migration path No fixed release		
12.1EV		Not Vulnerable		
12.1EW		Not Vulnerable		
12.1EX		Not Vulnerable		
12.1EY		Not Vulnerable		
12.1EZ		Vulnerable Not yet migrated No rebuild planned		
12.1T	Element	12.1(5)T17		Migrate to 12.2(19)b
	NAT	12.1(5)T17		Migrate to 12.2(19)b
	IPFW	12.1(5)T17		Migrate to 12.2(19)b
12.1X(l)	12.1X releases generally migrate to 12.1T, 12.2 or 12.2T as specified below. Please refer to specific train technical notes for documented migration path.			
12.1XA		Vulnerable. Migrate to 12.2(19)b		
12.1XB		Vulnerable. Migrate to 12.2(15)T5		
12.1XC		Vulnerable. Migrate to 12.2(19)b		
12.1XD		Vulnerable. Migrate to 12.2(19)b		
12.1XF		Not Vulnerable		
12.1XG		Vulnerable. Migrate to 12.2(15)T5		
12.1XH		Vulnerable. Migrate to 12.2(19)b		
12.1XI		Vulnerable. Migrate to 12.2(19)b		
12.1XJ		Vulnerable. Migrate to 12.2(15)T5		
12.1XL		Vulnerable. Migrate to 12.2(15)T5		
12.1XM		Vulnerable. Migrate to 12.2(2)XB15		

12.1XP		Vulnerable. Migrate to 12.2(15)T5		
12.1XQ		Vulnerable. Migrate to 12.2(2)XB15		
12.1XR		Vulnerable. Migrate to 12.2(15)T5		
12.1XT		Vulnerable. Migrate to 12.2(15)T5		
12.1XU		Vulnerable. Migrate to 12.2(4)T6		
12.1XV		Vulnerable. Migrate to 12.2(2)XB15		
12.1XW		Vulnerable. Migrate to 12.2(15)T5		
12.1YB		Vulnerable. Migrate to 12.2(15)T5		
12.1YC		Vulnerable. Migrate to 12.2(15)T5		
12.1YD		Vulnerable. Migrate to 12.2(15)T5		
12.1YE		Vulnerable. Migrate to 12.2(15)T5		
12.1YF		Vulnerable. Migrate to 12.2(15)T5		
12.1YH		Vulnerable. Migrate to 12.2(15)T5		
12.1YI		Vulnerable. Migrate to 12.2(15)T5		
12.1YJ		Not Vulnerable		
12.2-based Releases		Rebuild	Interim	Maintenance
12.2	Element	12.2(10g), 12.2(13c), 12.2(16a)		12.2(17)
	NAT	12.2(19b) 12.2(21a) 12.2(10g), 12.2(13e), 12.2(16f), 12.2(17d) - available by 16-Jan-2004		
	IPFW	Not Vulnerable		
12.2B		Migrate to 12.3(4)T		
12.2BC		Not Vulnerable		
12.2BW		Migrate to 12.2(15)T5		Migrate to 12.3(3e)
12.2BX		Vulnerable No migration path		
12.2BZ		Not Vulnerable		
12.2CX		Not Vulnerable		
12.2CY		Not Vulnerable		
12.2DA		Not Vulnerable		

12.2DD		Vulnerable. Migrate to 12.3(3e)		
12.2DX		Vulnerable. Migrate to 12.3(3e)		
12.2JA		Not Vulnerable		
12.2MB		Not Vulnerable		
12.2MC		Vulnerable No planned release		
12.2MX		Vulnerable. Migrate to 12.3(4)T1		
12.2S	Element	12.2(14)S3		12.2(18)S
	NAT	12.2(14)S7 available Feb-23-2004 12.2(18)S3 available Jan-19-2004		
	IPFW	Not Vulnerable		
12.2SX	Element	12.2(17a)SXA		
	NAT	12.2(17a)SXA		
	IPFW	TBD		
12.2SY		12.2(14)SY3		
12.2SZ		Not Vulnerable		
12.2T	Element	12.2(4)T6, 12.2(8)T10, 12.2(11)T9, 12.2(13)T5, 12.2(15)T2		No more maintenance trains for 12.2T are planned. Please migrate to the latest 12.3 Mainline release.
	NAT	12.2(4)T6, 12.2(8)T10, 12.2(11)T8, 12.2(13)T3, 12.2(15)T5		No more maintenance trains for 12.2T are planned. Please migrate to the latest 12.3 Mainline release.

	IPFW	12.2(4)T8		No more maintenance trains for 12.2T are planned. Please migrate to the latest 12.3 Mainline release.
12.2XA		Vulnerable. Migrate to 12.2(11)T9		
12.2XB	Element	12.2(2)XB14		
	NAT	12.2(2)XB14		
	IPFW	12.2(2)XB15		
12.2XC		Vulnerable. Migrate to 12.3(3e)		
12.2XD		Vulnerable. Migrate to 12.2(15)T5		
12.2XE		Not Vulnerable		
12.2XF		Not Vulnerable		
12.2XG		Vulnerable. Migrate to 12.2(8)T10		
12.2XH		Vulnerable. Migrate to 12.2(15)T5		
12.2XI		Vulnerable. Migrate to 12.2(15)T5		
12.2XJ		Vulnerable. Migrate to 12.2(15)T5		
12.2XK		Vulnerable. Migrate to 12.2(15)T5		
12.2XL		Vulnerable. Migrate to 12.2(15)T5		
12.2XM		Vulnerable. Migrate to 12.2(15)T5		
12.2XN		Vulnerable. Migrate to 12.2(11)T9		
12.2XQ		Vulnerable. Migrate to 12.2(15)T5		
12.2XS		Vulnerable. Migrate to 12.2(2)XB15		
12.2XT		Vulnerable. Migrate to 12.2(11)T9		
12.2XU		Vulnerable. Migrate to 12.2(15)T5		
12.2XW		Vulnerable. Migrate to 12.2(15)T5		
12.2YA	Element	12.2(4)YA7		
	NAT	Not Vulnerable		
	IPFW	12.2(4)YA8		
12.2YB		Vulnerable. Migrate to 12.2(15)T5		
12.2YC		Vulnerable. Migrate to 12.2(15)T5		
12.2YD		Vulnerable. Migrate to 12.3(2)T3		
12.2YE		Vulnerable. Migrate to 12.2(15)T5		
12.2YF		Vulnerable. Migrate to 12.2(15)T5		

12.2YG		Not Vulnerable		
12.2YH		Vulnerable. Migrate to 12.2(15)T5		
12.2YJ		Vulnerable. Migrate to 12.2(15)T5		
12.2YK		Vulnerable. Migrate to 12.2(13)ZC		
12.2YL		Vulnerable. Migrate to 12.3(2)T3		
12.2YM		Vulnerable. Migrate to 12.3(2)T3		
12.2YN		Vulnerable. Migrate to 12.3(2)T3		
12.2YO		Not Vulnerable		
12.2YP		Not Vulnerable		
12.2YQ		Not Vulnerable		
12.2YR		Not Vulnerable		
12.2YS		Not Vulnerable		
12.2YT		Vulnerable. Migrate to 12.2(15)T5		
12.2YU		Vulnerable. Migrate to 12.3(4)T1		
12.2YV		Vulnerable. Migrate to 12.3(4)T1		
12.2YW	Element	12.2(8)YW3		
	NAT	12.2(8)YW3		
	IPFW	Not Vulnerable		
12.2YX		Migrate to 12.2(S) Release 3 or migrate to 12.2(14)SU March-2004		
12.2YY		Vulnerable Migrate to 12.3(2)T3		
12.2YZ		Vulnerable. Rebuilds available upon request.		
12.2ZA		Not Vulnerable		
12.2ZB		Vulnerable Migrate to 12.3(2)T3		
12.2ZC		Vulnerable Not yet planned		
12.2ZD		Vulnerable No Migration path No planned fix		
12.2ZE		Vulnerable. Migrate to 12.3(3e)		
12.2ZF		Vulnerable. Migrate to 12.2(15)SL1		

12.2ZG		Vulnerable No Migration path No planned fix		
12.2ZH	Element	12.2(13)ZH3		
	NAT			
	IPFW	Not Vulnerable		
12.2ZJ	Element	12.2(15)ZJ3		
	NAT	12.2(15)ZJ2		
	IPFW	Not Vulnerable		
12.2ZL	Element	12.2(15)ZL1		
	NAT			
	IPFW	Not Vulnerable		
12.2ZM		Not Vulnerable		
12.2ZP		Not Vulnerable		
12.3-based Releases		Rebuild	Interim	Maintenance
12.3		Not Vulnerable		
12.3T	Element	Not Vulnerable to H.323 endpoint/gateway/gatekeeper issues		
	NAT	12.3(2)T3		
		12.3(4)T1		
IPFW	Not Vulnerable to IOS FW issue			

Cisco Software - Non IOS

In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco TAC for assistance as shown in the [Obtaining Fixed Software](#) section.

Cisco CallManager

Cisco CallManager Version	First Fixed Regular Release
3.1	3.1(4b)spD
3.2	3.2(3)
3.3	3.3(2)spC
	3.3(3)

Cisco Conference Connection

There are currently no software fixes planned for Cisco Conference Connection (CCC). Customers running CCC should implement a workaround to limit H.323 traffic from trusted hosts only. A workaround for this may be found in the [Workarounds](#) section.

Cisco Internet Service Node

There are currently no software fixes planned for Cisco Internet Service Node (ISN). Customers running ISN should implement a workaround to limit H.323 traffic from trusted hosts only. A workaround for this may be found in the [Workarounds](#) section.

Cisco 7905 Series IP Phone

These defects have been resolved in Version 1.0(1) of the 7905 H.323 phone firmware load. The version 1.0(1) image names containing the fixes are cp790501001h323031212a.sbin for the signed image and cp790501001h323031212a.zup for the unsigned image.

Cisco ATA18x Series Analog Telephony Devices

These defects have been resolved in software version 3.1.2.

Cisco BTS 10200

The Cisco BTS 10200 has software fixes available in version 4.1. Customers who have deployed the BTS 10200 should follow the instructions below in the [Obtaining Fixed Software](#) section to contact TAC in order to obtain the fixed software version.

Obtaining Fixed Software

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 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 assistance with the upgrade, which should be free of charge.

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

See <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.

Please 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.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Workarounds

Workarounds for H.323 endpoint and proxy configurations

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.

The Voice over IP SAFE paper talks about a variety of best practices that should keep your voice network isolated from the Internet. This reduces the risk of exposure, although attacks from within the local network should always be considered a potential risk.

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801b7a50.shtml

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

```

Workarounds for IOS devices performing NAT on H.323 traffic

Cisco IOS devices that run an affected version of 12.1 or 12.1E code and are configured to do static NAT are vulnerable to attacks with corrupted packets being processed by NAT through the device. There are several methods of reducing or removing the risk in these circumstances.

- **Access lists for the outside interface**

H.323 deep packet inspection is only done on packets with a source or destination port of 1720. If it is not necessary to translate or accept these packets, they can be blocked by an external device such as a firewall, or by input access lists applied to the outside interface of the device performing the NAT.

```

interface serial 0/0
 ip nat outside

!--- This is used to indicate which interface
!--- this configuration should be applied to.

ip access-group 101 in
!
access-list 101 deny tcp any eq 1720 any
access-list 101 deny tcp any any eq 1720
access-list 101 permit ip any any

```

- **Policy-based routing to block port 1720 traffic on static NAT translations**

Simple static translations allow through traffic on any port. If it is not necessary to allow H.323 traffic through your static NAT configuration, but applying access lists to your outside interface is not practical, you may use

policy-based routing to reroute traffic destined for port 1720. Policy-based routing is processed before NAT. In this example, the address 1.0.0.5 is an externally routable address for which the router is performing NAT to a local network address.

```
interface Null0
  no ip unreachable
  !
interface Ethernet0/0
  ip address 10.0.0.8 255.255.255.0
  ip nat inside
  !
interface Ethernet0/1
  ip address 11.0.0.8 255.255.255.0
  ip nat outside
  ip policy route-map block-h323

ip nat inside source static 10.0.0.5 1.0.0.5

access-list 102 permit tcp any host 1.0.0.5 eq 1720
access-list 102 permit tcp any eq 1720 host 1.0.0.5

route-map block-h323 permit 10
  match ip address 102
  set interface Null0
```

- **Blocking port 1720 using dynamic translations**

Dynamic translations are vulnerable to attack from the outside address of the original flow through the open translation, but can be timed out quickly to reduce the risk of exposure with the **ip nat translation port-timeout tcp 1720 2** command. This times out the translation for port 1720 in 2 seconds, and may be too short for the necessary call setup request to process.

NAT can be configured to not translate traffic sourced or destined to port 1720 with the use of route maps to match traffic instead of access lists. The sample configuration listed below permits traffic sourced from the 10.0.0.0/24 network to be translated to an address within the NAT pool "h323-test" except for traffic with a source or destination port of 1720.

Note: This will prevent users from using NAT for H.323-enabled applications from their PC desktops, such as NetMeeting. It is critical to understand your network and the applications in use on it when applying this type of workaround.

```
interface Ethernet0/0
  ip address 10.0.0.8 255.255.255.0
  ip nat inside
  !
interface Ethernet0/1
  ip address 11.0.0.8 255.255.255.0
  ip nat outside

ip nat pool h323-test 1.0.0.5 1.0.0.15 prefix-length 24
ip nat inside source route-map h323-block pool h323-test

access-list 101 deny    tcp any any eq 1720
access-list 101 deny    tcp any eq 1720 any
access-list 101 permit ip host 10.0.0.0 0.0.0.255

route-map h323-block permit 10
  match ip address 101
```

Defining a Windows-based access control list to limit H.323 traffic from only locally trusted hosts

There is an executable file available here named IPSec-H323.exe that contains scripts to aid in the configuration of access lists for Microsoft Windows 2000-based servers:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des?psrtdcat20e2>

This workaround has been tested to work with both Cisco Conference Connection and Internet Service Node to block potentially harmful H.323 packets. Please consult the IPSec-H323-Readme.htm file that is also available at the above link for further details regarding the scripts.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any malicious exploitation of any of the vulnerabilities described in this advisory.

These vulnerabilities were discovered through the use of the PROTOS H.323 test suite developed by the OUSPG at the University of Oulu, Finland, in concert with NISCC Vulnerability Management Team, the UK Government CERT.

These vulnerabilities are present in other products not provided by Cisco, and this security advisory is being published simultaneously with announcements from the other affected organizations.

Status of This Notice: INTERIM

This is an interim advisory. Although Cisco cannot guarantee the accuracy of all statements in this advisory, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory. Should there be a change in the facts, Cisco may update this advisory.

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

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040113-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
- bugtraq@securityfocus.com
- full-disclosure@lists.netsys.com
- vulnwatch@vulnwatch.org
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

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.

Revision History

Revision 1.4	2004-October-08	Added a Bug ID to the Details section for the Cisco ATA18x Series Analog Telephony Devices description. Changed the software version in the Software Versions and Fixes section for the Cisco ATA18x Series Analog Telephony Devices description.
Revision 1.3	2004-January-16	Clarified syntax of show process cpu include CCH323 command in "Affected Products" section.
Revision 1.2	2004-January-15	Clarified nature of affected releases in "Summary" and "Affected Products" sections; updated IOS software table for 12.2XB, 12.0, 12.1, 12.2B, 12.2S, and 12.2E; updated software link for IPSec-H323.exe in "Workarounds" section.
Revision 1.1	2004-January-14	Under "Affected Products" section: Replaced "AS5xxx series platforms" with "IOS images with the "PLUS" feature set"; under "Cisco IOS Processing of H.323 Traffic", removed mention of AS5xxx platforms; updated note under "H.323 Endpoints" section; updated note under "Cisco IOS Processing of H.323 Traffic" section; updated IOS software table for 12.2XB, 12.1E, 12.2, and 12.0; changed all references of "Migrate to 12.2(19)" to "Migrate to 12.2(19)b"; under the "Workarounds" section, updated section on "Defining a Windows-based access control list to limit H.323

		traffic from only locally trusted hosts"; under "Exploitation and Public Announcements" section, replaced mention of "UNIRAS" with "NISCC Vulnerability Management Team"
Revision 1.0	2004-January-13	Initial public release.

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/warp/public/707/sec_incident_response.shtml. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt/>.

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

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).