

# Cisco Security Advisory: Vulnerability in Cisco IOS Embedded Call Processing Solutions

Document ID: 63708

Advisory ID: cisco-sa-20050119-itscme

<http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml>

## Revision 1.1

Last Updated 2005 January 27 2000 UTC (GMT)

For Public Release 2005 January 19 1500 UTC (GMT)

---

Please provide your feedback on this document.

---

**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

Cisco Internetwork Operating System (IOS®) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for the Cisco IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.

A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml>

Cisco has made free software upgrades available to address this vulnerability for all affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability is documented by Cisco bug ID CSCee08584.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

This issue affects all Cisco devices running any unfixed version of Cisco IOS code that supports, and is configured for ITS, CME or SRST.

A Cisco device running ITS or CME will have the following line in the configuration:

```
telephony-service
```

A Cisco device running SRST will have the following line in the configuration:

```
call-manager-fallback
```

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 IOS release 12.0(3) with an installed image name of C2500-IS-L:

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

The release train label is "12.0".

The next example shows a product running IOS release 12.3(6) with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.3(6), RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

## Products Confirmed Not Vulnerable

ITS, CME and SRST are IOS-only features. Devices that do not run IOS are not vulnerable.

## Details

More information about Cisco's IOS Telephony Service (ITS) and Cisco CallManager Express (CME) can be found here:

<http://www.cisco.com/en/US/products/sw/voicesw/ps4625/index.html>

More information on Cisco's Survivable Remote Site Telephony (SRST) can be found here:

<http://www.cisco.com/en/US/products/sw/voicesw/ps2169/index.html>

ITS, CME and SRST are features that allow a Cisco device running IOS to control IP Phones using the Skinny Call Control Protocol (SCCP). SCCP is the Cisco CallManager native signaling protocol.

Certain malformed packets sent to the SCCP port on an IOS device configured for ITS, CME or SRST may cause the target device to reload. This issue is documented in Cisco bug ID CSCee08584.

The following commands can be used to determine if ITS or CME are running. A device that does not have ITS or CME enabled will display:

```
Router#show telephony-service
telephony-service is not enabled
```

A device that has ITS or CME enabled will show something similar to:

```
Router#show telephony-service
CONFIG (Version=3.0)
=====
Cisco CallManager Express
ip source-address 192.168.1.1 port 2000
max-ephones 2
max-dn 2
max-conferences 8
max-redirect 5
time-format 12
date-format mm-dd-yy
keepalive 30
timeout interdigit 10
timeout busy 10
timeout ringing 180
edit DN through Web: disabled.
edit TIME through web: disabled.
Log (table parameters):
  max-size: 150
  retain-timer: 15
create cnf-files version-stamp Jan 01 2002 00:00:00
auto assign 1 to 2
local directory service: enabled.
```

The following commands can be used to determine if SRST is running. A device that does not have SRST enabled will display:

```
Router#show call-manager-fallback
Call-manager fallback is not enabled
```

A device that has SRST enabled will show something similar to:

```
Router#show call-manager-fallback
CONFIG
=====
ip source-address 192.168.1.1 port 2000
max-ephones 2
max-dn 4
huntstop
time-format 12
date-format mm-dd-yy
```

```

keepalive 30
interdigit timeout 10
busy timeout 10
Limit number of DNS per phone:
  7910: 34
  7935: 34
  7940: 34
  7960: 34

```

Spoofed attacks are impractical since the attacker must pass all of the TCP/IP integrity checks first, including the initial sequence number and source TCP port number.

## Impact

Successful exploitation of the vulnerability may result in a device reload. Repeated exploitation could result in a Denial of Service (DoS) attack.

## Software Versions and Fixes

Each row of the Cisco IOS software table (below) 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 (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. 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. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For further information on the terms "Rebuild" and "Maintenance" please consult the following URL:

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

When considering software upgrades, please also consult [http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html) 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") for assistance.

Major Release	Availability of Repaired Releases	
<b>Affected 12.1-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.1YD	Migrate to 12.2(15)T13 or later	
12.1YE	Migrate to 12.2(15)T13 or later	
12.1YI	Migrate to 12.2(15)T13 or later	
<b>Affected 12.2-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>

12.2B	Migrate to 12.3(8)T or later	
12.2BC	Migrate to 12.3(9)BC or later	
12.2CZ	Migrate to 12.2(15)CZ1 or later	
12.2JK	12.2(15)JK2	
12.2T	12.2(13)T14	
	12.2(15)T13	
12.2XB	Migrate to 12.3(9) or later	
12.2XG	Migrate to 12.2(15)T13 or later	
12.2XM	Migrate to 12.2(15)T13 or later	
12.2XT	Migrate to 12.2(15)T13 or later	
12.2XU	Migrate to 12.2(15)T13 or later	
12.2XW	Migrate to 12.2(15)T13 or later	
12.2XZ	Migrate to 12.2(15)T13 or later	
12.2YA	12.2(4)YA8	
12.2YB	Migrate to 12.2(15)T13 or later	
12.2YC	Migrate to 12.2(15)T13 or later	
12.2YD	Migrate to 12.3(8)T or later	
12.2YF	Migrate to 12.2(15)T13 or later	
12.2YG	Migrate to 12.2(15)T13 or later	
12.2YH	Migrate to 12.2(15)T13 or later	
12.2YJ	Migrate to 12.2(15)T13 or later	
12.2YL	Migrate to 12.3(8)T or later	
12.2YM	Migrate to 12.3(8)T or later	
12.2YN	Migrate to 12.3(8)T or later	
12.2YQ	Migrate to 12.3(8)T or later	
12.2YR	Migrate to 12.3(8)T or later	
12.2YS	Migrate to 12.3(8)T or later	
12.2ZJ	Migrate to 12.3(4)T6 or later	
12.2ZK	Migrate to 12.3(8)T or later	
12.2ZO	Migrate to 12.2(15)T13 or later	
12.2ZP	Migrate to 12.3(4)XN2 or later	
<b>Affected 12.3–Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.3	12.3(5d)	
	12.3(6c)	

		12.3(9)
12.3T	12.3(2)T7	
	12.3(4)T6	
	12.3(7)T1	
		12.3(8)T
12.3XA	Migrate to 12.3(8)T or later	
12.3XB	Migrate to 12.3(8)T or later	
12.3XC	Migrate to 12.3(8)T or later	
12.3XD	12.3(4)XD3	
12.3XE	12.3(2)XE1	
12.3XF	Migrate to 12.3(11)T or later	
12.3XG	12.3(4)XG2	
12.3XH	Migrate to 12.3(11)T or later	
12.3XI		12.3(7)XI
12.3XJ	12.3(7)XJ2	
12.3XK	12.3(4)XK1	
12.3XL		12.3(7)XL
12.3XN	Contact Cisco TAC	
12.3XQ	12.3(4)XQ1 Release date not yet determined	

## Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

Affected devices that must run ITS, CME or SRST 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 ITS, CME or SRST traffic and putting firewalls in strategic locations may greatly reduce exposure until an upgrade can be performed.

The IP Telephony Security in Depth SAFE paper at the URL below discusses a variety of best practices that should keep your voice network isolated from the Internet. These best practices may help to reduce 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\\_papers\\_list.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_papers_list.html)

## Using 'strict-match'

It is possible to restrict SCCP communications to the IP specified in the **ip source-address** configuration

command by using the *strict-match* option. More information on this command can be found at the following URL:

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking\\_solutions\\_design\\_guidance09186a00801f8](http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8)

## Using Access Lists

Where possible, it is recommended to block SCCP traffic at the network edge with an Infrastructure Access Control List (iACL) or a Transit Access Control List (tACL).

For more information on iACLs, refer to "Protecting Your Core: Infrastructure Protection Access Control Lists":

<http://www.cisco.com/warp/public/707/iacl.html>

For more information on tACLs, refer to "Transit Access Control Lists: Filtering at Your Edge":

<http://www.cisco.com/warp/public/707/tacl.html>

Below is an example of an access list to block SCCP traffic from anywhere but a permitted network.

**Note:** In SRST deployments the SCCP packets are not addressed directly to the SRST device. The SCCP packets will be addressed to the call control devices (typically Cisco CallManager).

In this example, the permitted telephony devices are on the 172.16.0.0/16 network and the SCCP port being used is the default, TCP port 2000. If the specific IP addresses of the telephony devices are known, then the access list can be made to restrict traffic from only those devices.

```
!--- Permit access from any IP address in the 172.16.0.0/16
!--- to TCP port 2000.

access-list 101 permit tcp 172.16.0.0 0.0.255.255 any eq 2000

!--- Deny all traffic to port 2000.

access-list 101 deny tcp any any eq 2000

!--- Permit all other traffic.

access-list 101 permit ip any any
```

## Using Control Plane Policing

The Control Plane Policing (CoPP) feature may be used to mitigate this vulnerability. In the following example SCCP traffic is permitted to and from the 192.168.10.0/24 subnet. All other TCP port 2000 traffic destined to the device is blocked.

```
access-list 140 deny tcp 192.168.10.0 0.0.0.255 any eq 2000
access-list 140 deny tcp any 192.168.10.0 0.0.0.255 eq 2000
access-list 140 permit tcp any any eq 2000
```

```
access-list 140 deny ip any any

class-map match-all sccp-class
  match access-group 140

policy-map control-plane-policy
  class sccp-class

    police 8000 1500 1500 conform-action drop exceed-action drop

control-plane
  service-policy input control-plane-policy
```

CoPP is available in IOS release trains 12.2S and 12.3T. Additional information on the configuration and use of the CoPP feature can be found at the following URL:

[http://www.cisco.com/en/US/products/ps6642/products\\_white\\_paper0900aecd804fa16a.shtml](http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml)

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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.

## Exploitation and Public Announcements

The vulnerability described by CSCee08584 was originally reported to Cisco by SecureTest. The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

## 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.

## Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.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 (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-voice@puck.nether.net
- full-disclosure@lists.netsys.com
- 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.

## Revision History

Revision 1.1	2005-Jan-27	Added Release 12.2ZJ to Software Versions and Fixes table.
Revision 1.0	2005-Jan-19	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/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>.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jan 27, 2005

Document ID: 63708

---