

# Cisco Security Advisory: Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities

Advisory ID: cisco-sa-20090325-mobileip

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

## Revision 1.3

Last Updated 2009 June 25 2200 UTC (GMT)

For Public Release 2009 March 25 1600 UTC (GMT)

---

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

---

## Contents

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

## Summary

Devices that are running Cisco IOS Software and configured for Mobile IP Network

Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at the following link

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

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

Individual publication links are listed below:

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

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

## ☐ Affected Products

Devices that are running an affected version of Cisco IOS Software and configured for Mobile IP NAT Traversal feature or Mobile IPv6 are vulnerable.

### ☐ Vulnerable Products

Devices running Cisco IOS Software and configured for Mobile IP NAT Traversal feature will have a line similar to the following in the output of the **show running-config** command:

```
ip mobile home-agent nat traversal [...]
```

or

```
ip mobile foreign-agent nat traversal [...]
```

or

```
ip mobile router-service collocated registration nat traver
```

Devices running Cisco IOS Software and configured for Mobile IPv6 will have a line similar to the following in the output of the **show running-config** command:

```
ipv6 mobile home-agent
```

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),
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)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

*!--- output truncated*

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

## ▣ Products Confirmed Not Vulnerable

Cisco IOS XR is not affected by these vulnerabilities.

Cisco IOS XE is not affected by these vulnerabilities.

No other Cisco products are currently known to be affected by these vulnerabilities.

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

## ▣ Details

Mobile IP is part of both IPv4 and IPv6 standards. Mobile IP allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between different networks, connectivity at the different points is achieved seamlessly without user intervention. Roaming from a wired network to a wireless or wide-area network is also possible.

More information on Mobile IPv6 can be found at the following link: <http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mobile.html>

The Mobile IP Support NAT Traversal feature is documented in RFC 3519. It introduces an alternative method for tunneling Mobile IP data traffic. New extensions in the Mobile IP registration request and reply messages have been added for establishing User Datagram Protocol (UDP) tunneling. This feature allows mobile devices in collocated mode that use a private IP address (RFC 1918)

or foreign agents (FAs) that use a private IP address for the care-of address (CoA) to establish a tunnel and traverse a NAT-enabled router with mobile node (MN) data traffic from the home agent (HA).

More information on Mobile IP NAT Traversal feature can be found at the following link:

[http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t8/feature/guide/gtnatmip.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtnatmip.html)

Devices that are running an affected version of Cisco IOS Software and configured for Mobile IPv6 or Mobile IP NAT Traversal feature are affected by a DoS vulnerability. A successful exploitation of this vulnerability could cause an interface to stop processing traffic until the system is restarted. Offending packets need to be destined to the router for a successful exploit.

These vulnerabilities are documented in the Cisco Bug IDs [CSCsm97220](#) ([registered](#) customers only) and [CSCso05337](#) ([registered](#) customers only) and have been assigned Common Vulnerabilities and Exposures (CVE) IDs CVE-2009-0633 and CVE-2009-0634.

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

## ▣ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 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>.

**CSCsm97220 - Input queue wedged by MIPv6 packets**

**Calculate the environmental score of [CSCsm97220](#)**

<b>CVSS Base Score - 7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
<b>CVSS Temporal Score - 6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<b>CSCso05337 - HA: Input queue wedged by ICMP packet</b>					
<b>Calculate the environmental score of <a href="#">CSCso05337</a></b>					
<b>CVSS Base Score - 7.1</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
<b>CVSS Temporal Score - 5.9</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## ☐ Impact

Successful exploitation of the vulnerability may result in an interface to stop processing traffic, causing a 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 all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

<b>Major Release</b>	<b>Availability of Repaired Releases</b>	
<b>Affected 12.0-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.0 based releases		
<b>Affected 12.1-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.1 based releases		
<b>Affected 12.2-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.2 based releases		
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.3	Not Vulnerable	
12.3B	Not Vulnerable	
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	Not Vulnerable	
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	
12.3T	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3TPC	Not Vulnerable	
12.3VA	Not Vulnerable	
12.3XA	Not Vulnerable	
12.3XB	Not Vulnerable	
12.3XC	Not Vulnerable	
12.3XD	Not Vulnerable	
12.3XE	Not Vulnerable	
12.3XF	Not Vulnerable	
12.3XG	Not Vulnerable	
12.3XI	Not Vulnerable	
12.3XJ	Not Vulnerable	
12.3XK	Not Vulnerable	
12.3XL	Not Vulnerable	
12.3XQ	Not Vulnerable	
12.3XR	Not Vulnerable	
12.3XS	Not Vulnerable	
12.3XU	Not Vulnerable	
12.3XW	Not Vulnerable	
12.3XX	Not Vulnerable	
12.3XY	Not Vulnerable	
12.3XZ	Not Vulnerable	
12.3YA	Not Vulnerable	
12.3YD	Not Vulnerable	
12.3YF	Not Vulnerable	
12.3YG	Not Vulnerable	

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(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YM	12.3(14)YM13	12.3(14)YM13
12.3YQ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YS	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YU	Vulnerable; migrate to 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YX	Releases prior to 12.3(14)YX10 are vulnerable, release 12.3(14)YX10 and later are not vulnerable;	12.3(14)YX14
12.3YZ	Not Vulnerable	
12.3ZA	Not Vulnerable	

<b>Affected 12.4- Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	12.4(19)MR	12.4(19)MR2
12.4SW	Not Vulnerable	
12.4T	12.4(20)T 12.4(15)T8 12.4(15)T9; Available on 29- APR-2009	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XB	12.4(15)T8 12.4(20)T 12.4(15)T9; Available on 29- APR-2009	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
	Vulnerable; first	12.4(22)T1

12.4XC	fixed in <a href="#">12.4T</a>	12.4(15)T9; Available on 29- APR-2009
12.4XD	12.4(4)XD12; Available on 27- MAR-2009	12.4(4)XD12; Available on 27- MAR-2009
12.4XE	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1  12.4(15)T9; Available on 29- APR-2009
12.4XF	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1  12.4(15)T9; Available on 29- APR-2009
12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1  12.4(15)T9; Available on 29- APR-2009
12.4XK	Not Vulnerable	
12.4XL	12.4(15)XL4	12.4(15)XL4
12.4XM	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1  12.4(15)T9; Available on 29- APR-2009
12.4XN	Vulnerable; contact TAC	
12.4XP	Vulnerable; contact TAC	
12.4XQ	12.4(15)XQ2	12.4(15)XQ2
12.4XR	12.4(15)XR4	12.4(22)T1
12.4XT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1  12.4(15)T9; Available on 29- APR-2009
	Vulnerable;	

12.4XV	contact TAC	
12.4XW	12.4(11)XW10	12.4(11)XW10
12.4XY	12.4(15)XY4	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XZ	12.4(15)XZ1	12.4(15)XZ2
12.4YA	Not Vulnerable	
12.4YB	Not Vulnerable	
12.4YD	Not Vulnerable	

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

## Workarounds

The following mitigation and identification methods have been identified for these vulnerabilities:

### Infrastructure Access Control Lists

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

#### IPv4 example:

```
!--- Anti-spoofing entries are shown here.
```

```
!--- Deny special-use address sources.
```

```
!--- Refer to RFC 3330 for additional special use addresses.
```

```
access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
```

```
!--- Filter RFC 1918 space.
```

```
access-list 110 deny ip 10.0.0.0 0.255.255.255 any  
access-list 110 deny ip 172.16.0.0 0.15.255.255 any  
access-list 110 deny ip 192.168.0.0 0.0.255.255 any
```

```
!--- Deny your space as source from entering your AS.  
!--- Deploy only at the AS edge.
```

```
access-list 110 deny ip YOUR_CIDR_BLOCK any
```

```
!--- Permit BGP.
```

```
access-list 110 permit tcp host bgp_peer host router_ip eq bgp  
access-list 110 permit tcp host bgp_peer eq bgp host router_ip
```

```
!--- Deny access to internal infrastructure addresses.
```

```
access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES
```

```
!--- Permit transit traffic.
```

```
access-list 110 permit ip any any
```

## **IPv6 example:**

```
!--- Configure the access-list.
```

```
ipv6 access-list iacl
```

```
!--- Deny your space as source from entering your AS.  
!--- Deploy only at the AS edge.
```

```
deny ipv6 YOUR_CIDR_BLOCK_IPV6 any
```

```
!--- Permit multiprotocol BGP.
```

```

permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp
permit tcp host bgp_peer_ipv6 eq bgp host router_ipv6

```

*!--- Deny access to internal infrastructure addresses.*

```
deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6
```

*!--- Permit transit traffic.*

```
permit ipv6 any any
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_white\\_paper09186a00](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00)!

## Cisco IOS Embedded Event Manager

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

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

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

More information about EEM is available from Cisco.com at the following link:

[http://www.cisco.com/en/US/products/ps6815/products\\_ios\\_protocol\\_group\\_home](http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home).

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

## ☐ Obtaining Fixed Software

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

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software

upgrades, customers agree to be bound by the terms of Cisco's software license terms found at

[http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](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 reported to Cisco by a customer.

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

## ☐ **Status of this Notice: FINAL**

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

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

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

## ☐ **Distribution**

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

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.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 1.3	2009-June-25	Removed references to the March/09 combined fixed software table.
Revision 1.2	2009-June-1	Updated expected public availability date for release 12.4(23a).
Revision 1.1	2009-May-1	Updated expected public availability date for release 12.4(23a).
Revision 1.0	2009-Mar-25	Initial public release

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

## ☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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](#)

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