

# Cisco Security Advisory: Cisco IOS Software Multiple Features IP Sockets Vulnerability

Advisory ID: [cisco-sa-20090325-ip](#)

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

## Revision 1.4

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

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS<sup>®</sup> Software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.

The device may reload.

Cisco has released free software updates that address this vulnerability.

Several mitigation strategies are outlined in the "Workarounds" section of this advisory.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.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**

### ☐ **Vulnerable Products**

Devices that are running affected versions of Cisco IOS Software and Cisco IOS XE Software are affected if they are running any of the following features. Details about confirming whether the affected feature is enabled on a device are in the "Details" section of this advisory.

- Cisco Unified Communications Manager Express
- SIP Gateway Signaling Support Over Transport Layer Security (TLS) Transport
- Secure Signaling and Media Encryption
- Blocks Extensible Exchange Protocol (BEEP)
- Network Admission Control HTTP Authentication Proxy
- Per-user URL Redirect for EAPoUDP, Dot1x, and MAC Authentication Bypass
- Distributed Director with HTTP Redirects
- DNS (TCP mode only)

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 shows a product that is running Cisco IOS Software Release 12.4(20)T with an 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

The following products are not affected by this vulnerability:

- Cisco IOS XR Software
- Cisco 500 Series Wireless Express Access Points
- Cisco Aironet 1250 Series
- Cisco Aironet 1240 AG Series
- Cisco Aironet 1230 AG Series
- Cisco Aironet 1200 Series
- Cisco Aironet 1140 Series

### Cisco Aironet 1130 AG Series

- Cisco Aironet 1100 Series
- Cisco Aironet 1500 Series
- Cisco Aironet 1400 Series
- Cisco Aironet 1300 Series
- Cisco AP801 (in 860 and 880 series ISRs)
- Cisco WMIC (in Cisco 3200 MARs)

No other Cisco products or features configured in Cisco IOS or Cisco IOS XE Software are currently known to be affected by this vulnerability.

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

## Details

For successful exploitation of this vulnerability, the TCP three-way handshake must be completed to the associated TCP port number(s) for any of the features described in this section.

### Cisco Unified Communications Manager Express

The following configurations are vulnerable for different Cisco Unified Communications Manager Express services:

#### **A certificate authority proxy function (CAPF) server has been configured.**

The following example shows a vulnerable CAPF server configuration:

```
capf-server
auth-mode null-string
cert-enroll-trustpoint root password 1 104D000A061843595F
trustpoint-label cme_cert
source-addr 10.0.0.1
```

The default TCP port used for CAPF server is 3804.

Further information about CAPF-server is in the Cisco Unified Communications Manager Express System Administrator Guide at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucme/admin/configuration/guide/cmeauth.html#wp1085744](http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeauth.html#wp1085744).

#### **Telephony-service security parameters have been configured.**

If the telephony-service security parameters have been configured with "**device-security-mode**", the device is vulnerable. The following example shows three vulnerable configurations for telephony-service security parameters:

```
ephone 1
device-security-mode encrypted

ephone 2
device-security-mode authenticated

ephone 3
device-security-mode none
```

The TCP port used is defined with the "**ip source-address <address> port <port-number>**" telephony-service configuration command.

Further information about Telephony-service security parameters is in the Cisco Unified Communications Manager

Express System Administrator Guide at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucme/admin/configuration/guide/cmeauth.html#wp1080079](http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeauth.html#wp1080079).

### The global telephony-service or call-manager-fallback command has been configured.

Any Cisco IOS configuration with the global "**telephony-service**" or "**call-manager-fallback**" command is vulnerable if any subcommands are in the telephony-service or call-manager-fallback configuration mode. The following examples show vulnerable configurations:

```
telephony-service
ip source-address 192.168.0.1 port 2011
```

or

```
call-manager-fallback
ip source-address 192.168.0.1 port 2011
```

The TCP port used is defined with the "**ip source-address <address> port <port-number>**" configuration command.

Further information about telephony service and call-manager-fallback is in the Cisco Unified Communications Manager Express System Administrator Guide at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucme/admin/configuration/guide/cmestm.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmestm.html).

## SIP Gateway Signaling Support over TLS Transport

**Note:** For customers with devices enabled with SIP, also consult the document "Cisco Security Advisory: Cisco IOS Session Initiation Protocol Denial of Service Vulnerability" at the following link <http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml>.

Devices that are configured for SIP gateway signaling support over TLS transport are vulnerable. The following examples show vulnerable configurations:

```
voice service voip
sip
session transport tcp tls
url sips
```

-- or --

```
dial-peer voice 3456 voip
voice-class sip url sips
session protocol sipv2
session transport tcp tls
```

For the SIP gateway signaling support over TLS transport to function correctly, administrators must first configure a trustpoint using the following configuration:

```
sip-ua
crypto signaling default trustpoint example_trustpoint_name
```

The default TCP port used for the SIP gateway signaling support over TLS transport feature is 5061.

Further information about Cisco IOS SIP gateway signaling support over TLS transport is in the Cisco IOS Software Release 12.4T feature guide at [http://www.cisco.com/en/US/docs/ios/12\\_4t/12\\_4t11/FeatTLS.html](http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/FeatTLS.html).

## Secure Signaling and Media Encryption

A device is vulnerable if it is configured with the Media and Signaling Encryption (SRTP/TLS) on DSP Farm

Conferencing feature or with Secure Signaling and Media Encryption for analog phones with Skinny Call Control Protocol (SCCP).

The following examples show three different vulnerable secure DSP farm configurations. Several other parts are required for a full configuration, such as certificates and SCCP configuration, but these parts have been excluded for brevity.

```
dspfarm profile 2 transcode security
  trustpoint 2851ClientMina
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec gsmfr
  codec g729r8
  codec g729br8
  maximum sessions 3
  associate application SCCP

dspfarm profile 3 conference security
  trustpoint sec2800-cfb
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec g729r8
  codec g729br8
  maximum sessions 2
  associate application SCCP

dspfarm profile 5 mtp security
  trustpoint 2851ClientMina
  codec g711alaw
  maximum sessions hardware 1
  associate application SCCP
```

The default TCP port used for the Media and Signaling Encryption on DSP Farm Conferencing feature is **2443**.

Further information about the Media and Signaling Encryption on DSP Farm Conferencing feature is in the "Cisco IOS Software Release 12.4 Special and Early Deployments feature guide" at the following link [http://www.cisco.com/en/US/docs/ios/12\\_4t/12\\_4t15/itsdsp.html](http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/itsdsp.html).

The following output shows the relevant section of Secure Signaling and Media Encryption for analog phones and is a vulnerable configuration (Several other parts are required for a full configuration, such as certificates, SCCP configuration, and dial peers):

```
!--- The following lines show SCCP Telephony Control Application
!--- (STCAPP) security enabled at the system level:

stcapp ccm-group 1
stcapp security trustpoint analog
stcapp security mode encrypted
stcapp

<-- output removed for brevity -->

dial-peer voice 5002 pots
service stcapp

!--- The following line shows the security mode configured on the
!--- dial peer.

security mode authenticated
port 2/1
```

The default TCP port used for Media and Signaling Encryption for analog phones is **2443**.

Further information about Media and Signaling Encryption for analog phones is in the "Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide, Release 12.4T" at the following link [ht](#)

[tp://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/fsxsecur.html](http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/fsxsecur.html).

## Blocks Extensible Exchange Protocol

Any configuration or executable command that leverages Blocks Extensible Exchange Protocol (BEEP) as a transport protocol is vulnerable. The following example shows the vulnerable configuration of the feature NETCONF over BEEP. NETCONF over BEEP using SASL is also vulnerable.

```
crypto key generate rsa general-keys
crypto pki trustpoint my_trustpoint
enrollment url http://10.2.3.3:80
subject-name CN=dns_name_of_host.com
revocation-check none

crypto pki authenticate my_trustpoint
crypto pki enroll my_trustpoint

line vty 0 15
netconf lock-time 60
netconf max-sessions 16

netconf beep initiator host1 23 user my_user password
    my_password encrypt my_trustpoint
reconnect-time 60

netconf beep listener 23 sasl user1 encrypt my_trustpoint
```

The TCP port used is defined with the "**netconf beep initiator**" and "**netconf beep listener**" configuration commands.

Further information about NETCONF over BEEP is in the "Cisco IOS Software Release 12.4T feature guide" at the following link [http://www.cisco.com/en/US/docs/ios/12\\_4t/12\\_4t11/htnetbe.html#wp1049404](http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htnetbe.html#wp1049404).

The BEEP executable commands "**bingd**" and "**bingng**" could cause this vulnerability to be triggered when they are invoked. The following shows an example of these commands being executed:

```
bingng device 192.168.0.1 23
bingd device 23
```

## Network Admission Control HTTP Authentication Proxy

Devices configured with Network Admission Control HTTP Authentication Proxy are vulnerable. For the device to be vulnerable the authentication proxy rule must exist and be applied to an interface.

The following configuration creates an authentication proxy rule.

```
ip admission name example-ap-rule-name proxy http
```

The following configuration attaches the authentication proxy rule (created in the previous example) to an interface.

```
interface GigabitEthernet 0/0
ip admission example-ap-rule-name
```

The default TCP port used for Network Admission Control HTTP Authentication Proxy is **80**.

Further information about Network Admission Control HTTP Authentication Proxy is in the "Cisco IOS Security Configuration Guide, Release 12.4" at the following link [http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec\\_net\\_admsn\\_ctrl\\_external\\_dochbase\\_0900e4b1805b0530\\_4container\\_external\\_dochbase\\_0900e4b1807b01dc.html#wp1053991](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_net_admsn_ctrl_external_dochbase_0900e4b1805b0530_4container_external_dochbase_0900e4b1807b01dc.html#wp1053991).

## Per-user URL Redirect for EAPoUDP, Dot1x, and MAC Authentication Bypass

Devices that have URL redirect feature configured are vulnerable. URL redirect is supported for EAP over UDP (EAPoUDP), Dot1x and MAC Authentication Bypass (MAB) authentication mechanisms. The URL redirect configuration can either be on the server or set up as part of a locally defined profile or policy. Both configurations are vulnerable. A device is vulnerable with either of the following configurations.

### URL Redirect Feature Enabled for EAPoUDP

The URL redirect feature is enabled for EAPoUDP with the following global configuration command:

```
ip admission name <EAPoUDP-rule-name> eapoudp
```

The following configuration attaches the EAPoUDP rule (created in the previous example) to an interface.

```
ip admission name <EAPoUDP-rule-name>
```

### URL Redirect Feature Enabled for Dot1x and MAB

The URL redirect feature for both Dot1x and MAB are vulnerable and will have a URL redirect AV pair on the RADIUS server defined in a method that is similar to the following:

```
url-redirect="http://example.com"  
url-redirect="urlacl"
```

For the Dot1x and MAB URL redirect feature to work successfully on the switch, the minimum following configuration would also be required. There is no interface-specific configuration for URL redirect. Basically the interface has to be configured for Dot1x/MAB.

```
ip http {server | secure-server}  
ip device tracking
```

The default TCP port used for per-user URL redirect for EAPoUDP, Dot1x, and MAB is **80** and **443**.

Further information about per-user URL redirect for EAPoUDP, Dot1x, and MAB is in the "Catalyst 4500 Series Switch Software Configuration Guide, 12.2(50)SG" at the following link <http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/50sg/configuration/guide/dot1x.html#wp1311079>.

### Distributed Director with HTTP Redirects

A device is vulnerable if Distributed Director is configured with HTTP redirects. The following example shows a vulnerable configuration:

```
ip director ip-address 192.168.0.1
```

The default TCP port used for distributed director with HTTP redirect is **53**.

Further information about Distributed Director with HTTP redirects is in "Distributed Director Configuration Example Overview" at the following link [http://www.cisco.com/en/US/products/hw/contnetw/ps813/products\\_tech\\_note09186a00801fa9dd.shtml#topic8b](http://www.cisco.com/en/US/products/hw/contnetw/ps813/products_tech_note09186a00801fa9dd.shtml#topic8b).

### DNS

Devices that are configured with the Cisco IOS DNS feature are vulnerable. A pure DNS over UDP implementation is not vulnerable. See the "Workarounds" section of this advisory for information about filtering DNS over TCP traffic to the device. If **any** of the commands in the following example appear in the device configuration, the device is vulnerable:

```
ip dns server
```

```
ip dns primary example.com soa www.example.com admin@example.com
ip dns spoofing 192.168.0.1
```

The default TCP port used for DNS is **53**.

Further information about Cisco IOS DNS is in the "Cisco IOS IP Addressing Services Configuration Guide, Release 12.4" at the following link [http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad\\_config\\_dns\\_ps6350\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_config_dns_ps6350_TSD_Products_Configuration_Guide_Chapter.html).

This vulnerability is documented in the following Cisco Bug ID: [CSCsm27071](#) ([registered](#) customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifiers CVE-2009-0630.

[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>.

CSCsm27071: Cisco IOS Software Multiple Features IP Sockets Vulnerability					
Calculate the environmental score of <a href="#">CSCsm27071</a>					
CVSS Base Score - <b>7.8</b>					
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 may result in the any of the following occurring:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload.

Repeated attempts to exploit this vulnerability could result in a sustained 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.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
		12.4(18e)

12.0	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(23a); Available on 05-JUN-2009
12.0DA	Vulnerable; first fixed in <a href="#">12.2DA</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0DB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0DC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0S	12.0(32)S12	12.0(32)S12
12.0SC	Vulnerable; first fixed in <a href="#">12.0S</a>	12.0(32)S12
12.0SL	Vulnerable; first fixed in <a href="#">12.0S</a>	12.0(32)S12
12.0SP	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0ST	Vulnerable; first fixed in <a href="#">12.0S</a>	12.0(32)S12
12.0SX	Vulnerable; first fixed in <a href="#">12.0S</a>	12.0(32)S12
12.0SY	12.0(32)SY8	12.0(32)SY8

12.0SZ	Vulnerable; first fixed in <a href="#">12.0S</a>	12.0(32)S12
12.0T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0W	Vulnerable; contact TAC	
12.0WC	Vulnerable; contact TAC	
12.0WT	Not Vulnerable	
12.0XA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009

12.0XF	Not Vulnerable	
12.0XG	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XI	Releases prior to 12.0(4)XI2 are vulnerable, release 12.0(4)XI2 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XJ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XK	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XM	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009

12.0XN	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XQ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XR	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XS	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XT	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XV	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
<b>Affected 12.1- Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.1	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a);

		Available on 05-JUN-2009
12.1AA	Vulnerable; contact TAC	
12.1AX	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.1AY	Vulnerable; first fixed in <a href="#">12.1EA</a>	12.1(22)EA13 12.2(44)SE6
12.1AZ	Vulnerable; first fixed in <a href="#">12.1EA</a>	12.1(22)EA13 12.2(44)SE6
12.1CX	Vulnerable; contact TAC	
12.1DA	Vulnerable; first fixed in <a href="#">12.2DA</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1DB	Vulnerable; contact TAC	
12.1DC	Vulnerable; contact TAC	
12.1E	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF16
12.1EA	12.1(22)EA13	12.1(22)EA13
12.1EB	Vulnerable; contact TAC	
12.1EC	Vulnerable; first fixed in <a href="#">12.3BC</a>	12.2(33)SCB1 12.3(23)BC6

12.1EO	Vulnerable; contact TAC	
12.1EU	Vulnerable; first fixed in <a href="#">12.2SG</a>	12.2(31)SGA9
12.1EV	Vulnerable; contact TAC	
12.1EW	Vulnerable; migrate to 12.2SGA	
12.1EX	Vulnerable; contact TAC	
12.1EY	Vulnerable; contact TAC	
12.1EZ	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF16
12.1GA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1GB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
		12.4(18e)

12.1XB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(23a); Available on 05-JUN-2009
12.1XC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XF	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XG	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XI	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009

12.1XJ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XM	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XP	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XQ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XR	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XS	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
		12.4(18e)

12.1XT	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(23a); Available on 05-JUN-2009
12.1XU	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XV	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XW	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XX	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XY	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XZ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009

12.1YB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YE	Releases prior to 12.1(5)YE6 are vulnerable, release 12.1(5)YE6 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YF	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YI	Vulnerable; contact TAC	
12.1YJ	Vulnerable; first fixed in <a href="#">12.1EA</a>	12.1(22)EA13 12.2(44)SE6
<b>Affected</b>		

12.2- Based Releases	First Fixed Release	Recommended Release
12.2	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2B	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.2BC	Vulnerable; migrate to 12.2SCB1 or 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.2BW	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2BX	Vulnerable; migrate to 12.2SB4	12.2(33)SB4
12.2BY	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2BZ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2CX	Vulnerable; migrate to 12.2SCB or 12.3BC	12.2(33)SCB1 12.3(23)BC6

12.2CY	Vulnerable; migrate to 12.2SCB or 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.2CZ	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB4
12.2DA	12.2(12)DA14; Available on 30-JUL-2009	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2DD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2DX	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2EW	Vulnerable; first fixed in <a href="#">12.2SG</a>	12.2(31)SGA9
12.2EWA	Vulnerable; first fixed in <a href="#">12.2SG</a>	12.2(31)SGA9
12.2EX	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2EY	12.2(44)EY	12.2(44)SE6
12.2EZ	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2FX	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2FY	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6

12.2FZ	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2IRA	Vulnerable; first fixed in <a href="#">12.2SRC</a>	12.2(33)SRC4; Available on 18-MAY-2009
12.2IRB	Vulnerable; first fixed in <a href="#">12.2SRC</a>	12.2(33)SRC4; Available on 18-MAY-2009
12.2IXA	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2IXB	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2IXC	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2IXD	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2IXE	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2IXF	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2IXG	Vulnerable; migrate to any release in 12.2IXH	12.2(18)IXH; Available on 31-MAR-2009
12.2JA	Not Vulnerable	

12.2JK	Not Vulnerable	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.2MB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2MC	12.2(15)MC2m	12.2(15)MC2m
12.2S	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB4
12.2SB	12.2(31)SB14 12.2(33)SB1 12.2(28)SB13	12.2(33)SB4
12.2SBC	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB4
12.2SCA	12.2(33)SCA2	12.2(33)SCB1
12.2SCB	Not Vulnerable	
12.2SE	12.2(50)SE 12.2(46)SE2 12.2(44)SE5	12.2(44)SE6
12.2SEA	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2SEB	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2SEC	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6

12.2SED	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2SEE	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2SEF	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2SEG	Vulnerable; first fixed in <a href="#">12.2SE</a>	12.2(44)SE6
12.2SG	12.2(50)SG	12.2(52)SG; Available on 15-MAY-2009
12.2SGA	12.2(31)SGA9	12.2(31)SGA9
12.2SL	Not Vulnerable	
12.2SM	Vulnerable; contact TAC	
12.2SO	Vulnerable; contact TAC	
12.2SQ	Not Vulnerable	
12.2SRA	Vulnerable; first fixed in <a href="#">12.2SRC</a>	12.2(33)SRC4; Available on 18-MAY-2009
12.2SRB	Vulnerable; first fixed in <a href="#">12.2SRC</a>	12.2(33)SRB5a; Available on 3- April-2009  12.2(33)SRC4; Available on 18-MAY-2009
12.2SRC	12.2(33)SRC1	12.2(33)SRC4; Available on 18-MAY-2009

12.2SRD	Not Vulnerable	
12.2STE	Vulnerable; contact TAC	
12.2SU	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.2SV	Vulnerable; contact TAC	
12.2SVA	Vulnerable; contact TAC	
12.2SVC	Vulnerable; contact TAC	
12.2SVD	Vulnerable; contact TAC	
12.2SVE	Vulnerable; contact TAC	
12.2SW	Vulnerable; contact TAC	
12.2SX	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF16
12.2SXA	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF16
12.2SXB	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF16
12.2SXD	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF16
12.2SXE	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF16
12.2SXF	12.2(18)SXF16	12.2(18)SXF16

12.2SXH	12.2(33)SXH5; Available on 20-APR-2009	12.2(33)SXH5; Available on 20-APR-2009
12.2SXI	Not Vulnerable	
12.2SY	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB4
12.2SZ	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB4
12.2T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2TPC	Vulnerable; contact TAC	
12.2XA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009

12.2XE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XF	Vulnerable; migrate to 12.2SCB or 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.2XG	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XI	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XJ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XK	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009

12.2XM	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XN	Vulnerable; first fixed in <a href="#">12.2SRC</a>	12.2(33)SB4 12.2(33)SRD1
12.2XNA	Vulnerable; migrate to any release in 12.2SRD	12.2(33)SRD1
12.2XNB	Not Vulnerable	
12.2XNC	Not Vulnerable	
12.2XO	12.2(46)XO	12.2(46)XO
12.2XQ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XR	Not Vulnerable	
12.2XS	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XT	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
		12.4(18e)

12.2XU	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(23a); Available on 05-JUN-2009
12.2XV	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XW	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2YA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2YB	Vulnerable; contact TAC	
12.2YC	Vulnerable; contact TAC	
12.2YD	Vulnerable; contact TAC	
12.2YE	Vulnerable; contact TAC	
12.2YF	Vulnerable; contact TAC	
12.2YG	Vulnerable; contact TAC	
12.2YH	Vulnerable; contact TAC	
12.2YJ	Vulnerable; contact TAC	

12.2YK	Vulnerable; contact TAC	
12.2YL	Vulnerable; contact TAC	
12.2YM	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.2YN	Vulnerable; contact TAC	
12.2YO	Vulnerable; contact TAC	
12.2YP	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2YQ	Vulnerable; contact TAC	
12.2YR	Vulnerable; contact TAC	
12.2YS	Not Vulnerable	
12.2YT	Vulnerable; contact TAC	
12.2YU	Vulnerable; contact TAC	
12.2YV	Vulnerable; contact TAC	
12.2YW	Vulnerable; contact TAC	
12.2YX	Vulnerable; contact TAC	

12.2YY	Vulnerable; contact TAC	
12.2YZ	Vulnerable; contact TAC	
12.2ZA	Vulnerable; first fixed in <a href="#">12.2SXF</a>	12.2(18)SXF16
12.2ZB	Vulnerable; contact TAC	
12.2ZC	Vulnerable; contact TAC	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2ZF	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.2ZG	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.2ZH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2ZJ	Vulnerable; contact TAC	
12.2ZL	Vulnerable; contact TAC	

12.2ZP	Vulnerable; contact TAC	
12.2ZU	Vulnerable; first fixed in <a href="#">12.2SXH</a>	12.2(33)SXH5; Available on 20-APR-2009
12.2ZX	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB4
12.2ZY	Vulnerable; contact TAC	
12.2ZYA	12.2(18)ZYA1	12.2(18)ZYA1
<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(18e)  12.4(23a); Available on 05-JUN-2009
12.3B	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1  12.4(15)T9; Available on 29-APR-2009
12.3BC	12.3(23)BC6	12.3(23)BC6
12.3BW	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1  12.4(15)T9; Available on 29-APR-2009
12.3EU	Not Vulnerable	

12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	
12.3JK	Not Vulnerable	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3JL	Vulnerable; first fixed in <a href="#">12.4JK</a>	
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	Vulnerable; contact TAC	
12.3VA	Vulnerable; contact TAC	
12.3XA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3XB	Vulnerable; contact TAC	
12.3XC	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9;

		Available on 29-APR-2009
12.3XD	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3XF	Vulnerable; contact TAC	
12.3XG	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XI	Vulnerable; first fixed in <a href="#">12.2SB</a>	12.2(33)SB4
12.3XJ	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX14
12.3XK	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XL	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XQ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on

		29-APR-2009
12.3XR	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3XS	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XU	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XW	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX14
12.3XX	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XY	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3XZ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on

		29-APR-2009
12.3YD	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YF	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX14
12.3YG	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YH	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YI	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YK	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
		12.4(22)T1

12.3YQ	Vulnerable; first fixed in <a href="#">12.4T</a>	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; first fixed in <a href="#">12.4XB</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YX	12.3(14)YX14	12.3(14)YX14
12.3YZ	Vulnerable; contact TAC	
12.3ZA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
<b>Affected 12.4- Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	12.4(19) 12.4(18a) 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	Vulnerable; contact TAC	
12.4JMB	Vulnerable; contact TAC	
12.4JX	Not Vulnerable	
12.4MD	12.4(11)MD7	12.4(11)MD7
12.4MR	12.4(19)MR	12.4(19)MR2
12.4SW	Vulnerable; contact TAC	
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(22)T1 12.4(15)T9; Available on 29-APR-2009

12.4XC	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 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	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
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	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
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 12.4(15)T9; Available on 29-APR-2009
12.4XT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XV	Vulnerable; 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	Not Vulnerable	
12.4YA	Not Vulnerable	
12.4YB	Not Vulnerable	

12.4YD	Not Vulnerable	
--------	----------------	--

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

## Workarounds

The following mitigations have been identified for this vulnerability:

### 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:

```
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---
!--- Feature: Cisco Unified Communications Manager Express
!---
!--- CAPF server configuration
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 3804
```

```
!---
!--- Telephony-Service configuration
!--- The TCP port is as per the ip source-address
!--- <ip-address> port <port-number> telephony
!--- service configuration command. Example below 2999
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2999
```

```
!---
!--- Deny Cisco Unified Communications Manager Express traffic
!--- from all other sources destined to infrastructure addresses.
!---
```

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 3804
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2999
```

```
!---
!--- Feature: SIP Gateway Signaling Support Over TLS Transport
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 5061
```

```
!--- Deny SIP Gateway Signaling Support Over TLS Transport
!--- traffic from all other sources destined to infrastructure
!--- addresses.
```

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 5061
```

```
!---
!--- Feature: Secure Signaling and Media Encryption
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2443
```

```
!--- Deny Secure Signaling and Media Encryption traffic from all
!--- other sources destined to infrastructure addresses.
```

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 2443
```

```
!---
!--- Feature: Blocks Extensible Exchange Protocol (BEEP)
!--- The TCP port used is defined with the netconf beep initiator
!--- and netconf beep listener configuration
!--- commands. This example uses 3001
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 3001
```

```
!--- Deny BEEP traffic from all other sources destined to
!--- infrastructure addresses.
```

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 3001
```

```
!---
!--- Feature: Network Admission Control HTTP Authentication Proxy
!--- and
!--- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 80
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 443
```

```
!---
!--- Deny Network Admission Control HTTP Authentication Proxy
!--- and
!--- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!--- Authentication Bybass traffic to infrastructure
!---
```

```
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 80
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 443
```

```
!---
!--- Features: Distributed Director with HTTP Redirects and DNS
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
```

```
!--- Deny Distributed Director with HTTP Redirects traffic and DNS
!--- from all other sources destined to infrastructure addresses.
```

```

access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 53

!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and configurations
!--- Permit all other traffic to transit the device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example shown)

interface serial 2/0
ip access-group 150 in

```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_white\\_paper09186a00801a1a55.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml)

## Receive ACLs (rACL)

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 (GSR), 12.0(24)S for the 7500, and 12.0(31)S for the 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured. On the 12000, 7500, and 10720, transit traffic is never affected by a receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below only refer to the router's own physical or virtual IP addresses. Receive ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled "GSR: Receive Access Control Lists" will help you identify and allow legitimate traffic to your device and deny all unwanted packets. This white paper is available at the following link [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_white\\_paper09186a00801a0a5e.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml).

The following is the receive path ACL written to permit this type of traffic from trusted hosts:

```

!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---

!---
!--- Feature: Cisco Unified Communications Manager Express
!---
!---

!---
!--- Permit CAPF server traffic from trusted hosts allowed to
!--- the RP.
!---

access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 3804

!---
!--- Telephony-Service configuration
!---

!---
!--- The TCP port is as per the ip source-address
!--- <address> port <port-number> telephony-service
!--- configuration command. Example below 2999
!---
!--- Permit Telephony-Service traffic from trusted hosts allowed

```

```
!--- to the RP.
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 2999
```

```
!---  
!--- Deny Cisco Unified Communications Manager Express  
!--- traffic from all other sources to the RP.  
!---
```

```
access-list 150 deny tcp any any eq 3804  
access-list 150 deny tcp any any eq 2999
```

```
!---  
!--- Permit SIP Gateway Signaling Support Over TLS Transport  
!--- traffic from trusted hosts allowed to the RP.  
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 5061
```

```
!---  
!--- Deny SIP Gateway Signaling Support Over TLS Transport  
!--- traffic from all other sources to the RP.  
!---
```

```
access-list 150 deny tcp any any eq 5061
```

```
!---  
!--- Permit Secure Signaling and Media Encryption traffic  
!--- from trusted hosts allowed to the RP.  
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 2443
```

```
!---  
!--- Deny Secure Signaling and Media Encryption traffic from  
!--- all other sources to the RP.  
!---
```

```
access-list 150 deny tcp any any eq 2443
```

```
!---  
!--- Feature: Blocks Extensible Exchange Protocol (BEEP)  
!--- The TCP port used is defined with the netconf beep initiator  
!--- and netconf beep listener configuration commands.  
!--- This example uses 3001  
!---
```

```
!---  
!--- Permit BEEP traffic from trusted hosts allowed to the RP.  
!---
```

```
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 3001
```

```
!---  
!--- Deny BEEP traffic from all other sources to the RP.  
!---
```

```
access-list 150 deny tcp any any eq 3001
```

```

!----
!---- Feature: Network Admission Control HTTP Authentication Proxy
!---- and
!---- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!---- Authentication Bybass
!----

!----
!---- Permit Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!---- Authentication Bybass traffic from trusted hosts allowed to
!---- the RP.
!----

access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 80
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 443

!----
!---- Deny Network Admission Control HTTP Authentication Proxy
!---- and
!---- Per-user URL Redirect for EAP over UDP, Dot1x and MAC
!---- Authentication Bybass traffic from all other sources to
!---- the RP.
!----

access-list 150 deny tcp any any eq 80
access-list 150 deny tcp any any eq 443

!----
!---- Features: Distributed Director with HTTP Redirects and DNS
!----

!----
!---- Permit Distribute Director and DNS traffic from trusted hosts
!---- allowed to the RP.
!----

access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 53

!----
!---- Deny distributed director and DNS traffic from all other
!---- sources to the RP.
!----

access-list 150 deny tcp any any eq 53

!----
!---- Permit all other traffic to the RP.
!---- according to security policy and configurations.
!----

access-list 150 permit ip any any

!----
!---- Apply this access list to the 'receive' path.
!----

ip receive access-list 150

```

## Control Plane Policing

Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of

direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP which will protect all devices with IP addresses in the infrastructure IP address range.

```

!---
!--- Only sections pertaining to features enabled on the device
!--- need be configured.
!---
!--- Feature: Cisco Unified Communications Manager Express
!---
!--- CAPF Server configuration
!---

access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 3804

!---

!--- Telephony-Service configuration
!--- The TCP port is as per the ip source-address
!--- <address> port <port-number> telephony-service
!--- configuration command. Example below 2999
!---

access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 2999

!---
!--- Permit Cisco Unified Communications Manager Express traffic
!--- sent to all IP addresses configured on all interfaces of
!--- the affected device so that it will be policed and dropped
!--- by the CoPP feature
!---
!--- CAPF server configuration
!---

access-list 150 permit tcp any any eq 3804

!---
!--- Telephony-Service configuration
!---

access-list 150 permit tcp any any eq 2999

!---
!--- Feature: SIP Gateway Signaling Support Over TLS Transport
!---

access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 5061

!---
!--- Permit SIP Gateway Signaling Support Over TLS Transport
!--- traffic sent to all IP addresses configured on all interfaces
!--- of the affected device so that it will be policed and
!--- dropped by the CoPP feature
!---

access-list 150 permit tcp any any eq 5061

!---
!--- Feature: Secure Signaling and Media Encryption
!---

access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 2443

```

```
!----  
!---- Permit Secure Signaling and Media Encryption traffic sent to  
!---- all IP addresses configured on all interfaces of the affected  
!---- device so that it will be policed and dropped by the CoPP  
!---- feature  
!----
```

```
access-list 150 permit tcp any any eq 2443
```

```
!----  
!---- Feature: Blocks Extensible Exchange Protocol (BEEP)  
!---- The TCP port used is defined with the netconf beep initiator  
!---- and netconf beep listener configuration commands.  
!---- This example uses 3001  
!----
```

```
access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 3001
```

```
!----  
!---- Permit BEEP traffic sent to all IP addresses configured  
!---- on all interfaces of the affected device so that it  
!---- will be policed and dropped by the CoPP feature  
!----
```

```
access-list 150 permit tcp any any eq 3001
```

```
!----  
!---- Feature: Network Admission Control HTTP Authentication Proxy  
!---- and  
!---- Per-user URL Redirect for EAP over UDP, Dot1x and MAC  
!---- Authentication Bypass  
!----
```

```
access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 80  
access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 443
```

```
!----  
!---- Permit Network Admission Control HTTP Authentication Proxy  
!---- and Per-user URL Redirect for EAP over UDP, Dot1x and MAC  
!---- Authentication Bypass traffic sent to all IP addresses  
!---- configured on all interfaces of the affected device so that it  
!---- will be policed and dropped by the CoPP feature  
!----
```

```
access-list 150 permit tcp any any eq 80  
access-list 150 permit tcp any any eq 443
```

```
!----  
!---- Features: Distributed Director with HTTP Redirects and DNS  
!----
```

```
access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD  
any eq 53
```

```
!----  
!---- Permit Distributed Director with HTTP Redirects and DNS  
!---- traffic sent to all IP addresses configured on all interfaces  
!---- of the affected device so that it will be policed and dropped  
!---- by the CoPP feature  
!----
```

```
access-list 150 permit tcp any any eq 53
```

```

!----
!---- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!---- Layer4 traffic in accordance with existing security policies
!---- and configurations for traffic that is authorized to be sent
!---- to infrastructure devices
!----

!----
!---- Create a Class-Map for traffic to be policed by
!---- the CoPP feature
!----

class-map match-all drop-tcpip-class
match access-group 150

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

policy-map drop-tcpip-traffic

class drop-tcpip-class
drop

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

control-plane
service-policy input drop-tcpip-traffic

```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS trains:

```

policy-map drop-tcpip-traffic
class drop-tcpip-class
police 32000 1500 1500 conform-action drop exceed-action drop

```

Additional information on the configuration and use of the CoPP feature can be found in the documents, "Control Plane Policing Implementation Best Practices" and "Cisco IOS Software Releases 12.2 S - Control Plane Policing" at the following links [http://www.cisco.com/web/about/security/intelligence/coppwp\\_gs.html](http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html) and [http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t4/feature/guide/gtrtlimt.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html).

Additional mitigations that can be deployed on Cisco devices within the network are available in the "Cisco Applied Mitigation Bulletin" companion document for this advisory at the following link <http://www.cisco.com/warp/public/707/cisco-amb-20090325-tcp-and-ip.shtml>.

[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 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 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 discovered by Cisco when performing internal vulnerability testing. We would also like to thank Jens Link, freelance consultant, for also reporting this vulnerability to us.

[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-ip.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 1.4	2009- June-25	Removed references to the March/09 combined fixed software table.
Revision 1.3	2009- June-1	Updated expected public availability date for release 12.4(23a).
Revision 1.2	2009- May-1	Updated expected public availability date for release 12.4(23a).

Revision 1.1	2009-March-30	Specifically called out Wireless Products as not affected
Revision 1.0	2009-March-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](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)