

Cisco Security Advisory: Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability

Advisory ID: cisco-sa-20090325-sip

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

Revision 1.4

Last Updated 2009 June 26 1500 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 exists in the Session Initiation Protocol (SIP) implementation in Cisco

IOS Software that can be exploited remotely to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.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

This vulnerability only affects devices running Cisco IOS Software with SIP voice services enabled.

☐ Vulnerable Products

Cisco devices running affected Cisco IOS Software versions that process SIP messages are affected. The only requirement for this vulnerability is that the Cisco IOS device process SIP messages as part of configured VoIP functionality. Note that this does not apply to the processing of SIP messages as part of the NAT and firewall feature sets.

Recent versions of Cisco IOS Software do not process SIP messages by default. Creating a dial peer by way of the command **dial-peer voice** will start the SIP processes and cause the Cisco IOS device to start processing SIP messages. In addition, several features within Cisco Unified Communications Manager Express, such as ePhones, once configured will also automatically start the SIP process, which will cause the device to start processing SIP messages. An example of an affected configuration is as follows:

```
dial-peer voice <Voice dial-peer tag> voip
...
!
```

Note: Older versions of Cisco IOS Software were affected by a bug that caused Cisco IOS Software to process SIP messages without being configured for SIP operation. Refer to <http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml> for additional information on Cisco bug ID [CSCsb25337](#) ([registered customers only](#)) .

In addition to inspecting the Cisco IOS device configuration for a **dial-peer** command that causes the device to process SIP messages, administrators can also use the command **show processes | include SIP** to determine whether Cisco IOS Software is running the processes that handle SIP messages. In the following example, the presence of the processes **CCSIP_UDP_SOCKET** and **CCSIP_TCP_SOCKET** indicates that the Cisco IOS device is processing SIP messages:

```
Router#show processes | include SIP
 147 Mwe 40F46DF4          12      2    600023468,
 148 Mwe 40F21244           0      1         0 5524,
 149 Mwe 40F48254           4      1    400023108,
```

150 Mwe 40F48034

4

1

400023388,

Warning: Since there are several ways a device running Cisco IOS Software can start processing SIP messages, it is recommended that the **show processes | include SIP** command be used to determine whether the device is processing SIP messages instead of relying on the presence of specific configuration commands.

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), RELI
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

The SIP Application Layer Gateway (ALG), which is used by the Cisco IOS

NAT and firewall features of Cisco IOS Software, is not affected by this vulnerability.

Cisco devices that are running Cisco IOS XE Software and Cisco IOS XR Software are not affected.

No other Cisco products are currently known to be affected by this vulnerability.

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

☐ Details

SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

A denial of service (DoS) vulnerability exists in the SIP implementation in Cisco IOS Software. This vulnerability is triggered by processing a specific and valid SIP message.

This vulnerability is documented in Cisco Bug ID [CSCsu11522](#) ([registered customers only](#)) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-0636.

Note: The vulnerabilities described in the advisories [Cisco IOS Software Multiple Features IP Sockets Vulnerability](#) and [Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability](#), both part of this bundle of Cisco IOS advisories, may also impact SIP operations.

[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>.

CSCsu11522 - A voice gateway may crash when processing valid SIP message					
Calculate the environmental score of CSCsu11522					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

☐ Impact

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

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

☐ Software Versions and Fixes

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

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

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

Note: In addition to [CSCsu11522](#) and because of its impact on SIP operation, this table of fixed software takes into consideration the vulnerability tracked by Cisco Bug [CSCsk64158](#), from "Cisco Security Advisory: Crafted UDP Packet Affects Multiple Cisco IOS Features" (<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>.) The table does not take into consideration the vulnerability disclosed by "Cisco Security Advisory: Cisco IOS IP Sockets Vulnerability Affecting Multiple Cisco IOS Features", which may impact SIP over TLS.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
12.0	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0DA	Vulnerable; first fixed in 12.2DA	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0DB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0DC	Vulnerable; first fixed in 12.4	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 12.0S	12.0(32)S12
12.0SL	Vulnerable; first fixed in 12.0S	12.0(32)S12
12.0SP	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0ST	Vulnerable; first fixed in 12.0S	12.0(32)S12
12.0SX	Vulnerable; first fixed in 12.0S	12.0(32)S12
12.0SY	12.0(32)SY8	12.0(32)SY8
12.0SZ	Vulnerable; first fixed in 12.0S	12.0(32)S12
12.0T	Vulnerable; first fixed in 12.4	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 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XC	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-

		JUN-2009
12.0XD	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XE	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XF	Not Vulnerable	
12.0XG	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XH	Vulnerable; first fixed in 12.4	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 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XJ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XK	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XL	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-

		JUN-2009
12.0XM	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XN	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XQ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XR	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XS	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XT	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.0XV	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
12.1	Vulnerable; first	12.4(18e) 12.4(23a);

	fixed in 12.4	Available on 05-JUN-2009
12.1AA	Vulnerable; contact TAC	
12.1AX	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.1AY	Vulnerable; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
12.1AZ	Vulnerable; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
12.1CX	Vulnerable; contact TAC	
12.1DA	Vulnerable; contact TAC	
12.1DB	Vulnerable; contact TAC	
12.1DC	Vulnerable; contact TAC	
12.1E	Vulnerable; first fixed in 12.2SXF	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 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.1EO	Vulnerable; contact TAC	
12.1EU	Vulnerable; first fixed in 12.2SG	12.2(31)SGA9
12.1EV	Vulnerable; contact TAC	
12.1EW	Vulnerable; migrate to 12.2SGA	12.2(31)SGA9
	Vulnerable; first	12.4(18e)

12.1EX	fixed in 12.4	12.4(23a); Available on 05- JUN-2009
12.1EY	Vulnerable; contact TAC	
12.1EZ	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.1GA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.1GB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.1T	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.1XA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.1XB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.1XC	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.1XD	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009

12.1XE	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XF	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XG	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XH	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XI	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XJ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XL	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XM	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XP	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a);

		Available on 05-JUN-2009
12.1XQ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XR	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XS	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XT	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XU	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XV	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XW	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1XX	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
		12.4(18e)

12.1XY	Vulnerable; first fixed in 12.4	12.4(23a); Available on 05-JUN-2009
12.1XZ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YC	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YD	Vulnerable; first fixed in 12.4	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 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.1YF	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
	Vulnerable; first	12.4(18e)

12.1YH	fixed in 12.4	12.4(23a); Available on 05- JUN-2009
12.1YI	Vulnerable; contact TAC	
12.1YJ	Vulnerable; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
Affected 12.2- Based Releases	First Fixed Release	Recommended Release
12.2	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2B	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.2BC	Vulnerable; migrate to 12.2SCB or 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.2BW	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2BX	Vulnerable; migrate to 12.2SB	12.2(33)SB4
12.2BY	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2BZ	Vulnerable; first fixed in 12.4	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 12.2SB	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 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2DX	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2EW	Vulnerable; first fixed in 12.2SG	12.2(31)SGA9
12.2EWA	Vulnerable; first fixed in 12.2SG	12.2(31)SGA9
12.2EX	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2EY	12.2(44)EY	12.2(44)SE6
12.2EZ	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2FX	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2FY	Vulnerable; first fixed in 12.2SE	12.2(44)SE6

12.2FZ	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2IRA	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4; Available on 18-MAY-2009
12.2IRB	Vulnerable; first fixed in 12.2SRC	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	
12.2MB	Vulnerable; first fixed in 12.4	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 12.2SB	12.2(33)SB4
12.2SB	12.2(28)SB13	12.2(33)SB4
	12.2(31)SB14	
	12.2(33)SB3	
12.2SBC	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2SCA	Vulnerable; first fixed in 12.2SCB	12.2(33)SCB1
12.2SCB	12.2(33)SCB1	12.2(33)SCB1
12.2SE	12.2(50)SE	12.2(44)SE6
	12.2(46)SE2	
	12.2(44)SE5	
12.2SEA	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEB	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEC	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SED	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEE	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEF	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2SEG	Vulnerable; first fixed in 12.2SE	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	12.2(44)SQ1	
12.2SRA	Vulnerable; first fixed in 12.2SRC	12.2(33)SRD1 12.2(33)SRC4; Available on 18- MAY-2009
12.2SRB	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4; Available on 18- MAY-2009 12.2(33)SRD1 12.2(33)SRB5a; Available on 3- April-2009
12.2SRC	12.2(33)SRC4; Available on 18- MAY-2009	12.2(33)SRC4; Available on 18- MAY-2009
12.2SRD	Not Vulnerable	
12.2STE	Vulnerable; contact TAC	
12.2SU	Vulnerable; first fixed in 12.4T	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 12.2SXF	12.2(18)SXF16
12.2SXA	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXB	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXD	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXE	Vulnerable; first fixed in 12.2SXF	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 12.2SB	12.2(33)SB4
12.2SZ	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2T	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2TPC	Vulnerable; contact TAC	
12.2XA	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2XB	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
		12.4(18e)

12.2XC	Vulnerable; first fixed in 12.4	12.4(23a); Available on 05-JUN-2009
12.2XD	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XE	Vulnerable; first fixed in 12.4	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 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XH	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XI	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XJ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XK	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
		12.4(18e)

12.2XL	Vulnerable; first fixed in 12.4	12.4(23a); Available on 05-JUN-2009
12.2XM	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XN	Vulnerable; first fixed in 12.2SRC	12.2(33)SB4 12.2(33)SRD1
12.2XNA	Vulnerable; migrate to any release in 12.2SRD	12.2(33)SRD1
12.2XNB	12.2(33)XNB1	12.2(33)XNB3
12.2XNC	Not Vulnerable	
12.2XO	12.2(46)XO	12.2(46)XO
12.2XQ	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XR	Not Vulnerable	
12.2XS	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XT	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.2XU	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
	Vulnerable; first	12.4(18e)

12.2XV	fixed in 12.4	12.4(23a); Available on 05- JUN-2009
12.2XW	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009
12.2YA	Vulnerable; first fixed in 12.4	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 12.4T	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 12.4	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 12.2SXF	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 12.4	12.4(18e) 12.4(23a); Available on 05- JUN-2009

12.2ZF	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.2ZG	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.2ZH	Vulnerable; first fixed in 12.4	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 12.2SXH	12.2(33)SXH5; Available on 20-APR-2009
12.2ZX	Vulnerable; first fixed in 12.2SB	12.2(33)SB4
12.2ZY	Vulnerable; contact TAC	
12.2ZYA	12.2(18)ZYA1	12.2(18)ZYA1
Affected 12.3- Based Releases	First Fixed Release	Recommended Release
12.3	Vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3B	Vulnerable; first fixed in 12.4T	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 12.4T	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	
12.3JL	Vulnerable; contact TAC	
12.3JX	Not Vulnerable	
12.3T	Vulnerable; first fixed in 12.4T	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 12.4	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.3XB	Vulnerable; contact TAC	
12.3XC	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
		12.4(22)T1

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

		Available on 29- APR-2009
12.3XU	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.3XW	Vulnerable; first fixed in 12.3YX	12.3(14)YX14
12.3XX	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.3XY	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.3XZ	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.3YA	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.3YD	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.3YF	Vulnerable; first fixed in 12.3YX	12.3(14)YX14
12.3YG	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
		12.4(22)T1

12.3YH	Vulnerable; first fixed in 12.4T	12.4(15)T9; Available on 29-APR-2009
12.3YI	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YJ	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YK	Vulnerable; first fixed in 12.4T	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 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YS	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YT	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.3YU	Vulnerable; first fixed in 12.4XB	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 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
Affected 12.4- Based Releases	First Fixed Release	Recommended Release
12.4	12.4(18e) 12.4(23) 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)MR1	12.4(19)MR2
12.4SW	Vulnerable; contact TAC	
12.4T	12.4(20)T2 12.4(15)T8 12.4(22)T 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	12.4(22)T1 12.4(15)T9;

	fixed in 12.4T	Available on 29-APR-2009
12.4XB	12.4(15)T8 12.4(20)T2 12.4(15)T9; Available on 29-APR-2009	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XC	Vulnerable; first fixed in 12.4T	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 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XF	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XG	12.4(15)T8 12.4(20)T2	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XJ	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XK	Vulnerable; first fixed in 12.4T	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 12.4T	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 12.4T	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	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
12.4XZ	12.4(15)XZ2	12.4(15)XZ2
12.4YA	12.4(20)YA2	12.4(20)YA3
12.4YB	Not Vulnerable	
12.4YD	Not Vulnerable	

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

☐ Workarounds

If the affected Cisco IOS device requires SIP for VoIP services, SIP cannot be disabled, and therefore, no workarounds are available. Users are advised to apply mitigation techniques to help limit exposure to the vulnerability. Mitigation consists of allowing only legitimate devices to connect to the routers. To increase

effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS SIP and Crafted UDP Vulnerabilities", which is available at the following location:
<http://www.cisco.com/warp/public/707/cisco-amb-20090325-sip-and-udp.shtml>.

Disable SIP Listening Ports

For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to accomplish this with the following commands:

```
sip-ua
no transport udp
no transport tcp
```

Warning: When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

After applying this workaround, administrators are advised to use the **show** commands, as discussed in the [Affected Products](#) section of this advisory, to confirm that the Cisco IOS device is no longer processing SIP messages.

Control Plane Policing

For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to the network:

```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are tr
!-- Everything else is not trusted. The following access list
!-- to determine what traffic needs to be dropped by a contro
!-- policy (the CoPP feature.) If the access list matches (pe
!-- then traffic will be dropped and if the access list does
```

```

!-- match (deny) then traffic will be processed by the router

access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!-- 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-sip-class
  match access-group 100

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

policy-map drop-sip-traffic
  class drop-sip-class
    drop

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

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

```

Warning: Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of the sender, which may defeat access control lists that permit communication to these ports from trusted IP addresses.

In the above CoPP example, the access control 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. Additional information on the configuration and use of the CoPP feature can be found at 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.

[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, 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

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 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 during handling of customer service requests.

[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-sip.shtml>

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

news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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-26	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-April-03	Releases 12.2XR, 12.4JL, 12.4JK, 12.4JX, 12.4JDA, 12.4JA, 12.3JX, 12.3JK, 12.3JEC, 12.3JEB, 12.3JEA, 12.3JA, 12.2JA, and 12.2JK have been confirmed to be not vulnerable. Adjusted fixed software table accordingly.
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. 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)

☐

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

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

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