

Summary of Cisco IOS Software Bundled Advisories, September 22, 2010

Advisory ID: **cisco-sa-20100922-bundle**

<http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml>

Revision 1.0

For Public Release 2010 September 22 1600 UTC (GMT)

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

Contents

- [Summary](#)
- [Software Versions and Fixes](#)
- [Obtaining Fixed Software](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

The September 22, 2010, Cisco IOS® Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table below lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

This list also includes all individual publication links:

- Cisco IOS Software H.323 Denial of Service Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml>
- Cisco IOS Software Internet Group Management Protocol Denial of Service Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml>
- Cisco IOS Software Network Address Translation Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml>
- Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml>
- Cisco IOS SSL VPN Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-sslvpn.shtml>
- Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-cucmsip.shtml>

This summary page is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml>.

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

▣ 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 following Cisco IOS Software table corresponds to a Cisco IOS Software train. If a particular train is vulnerable, the First Fixed Release for All Advisories in the September 2010 Bundle Publication column lists the earliest possible releases that correct all the published vulnerabilities in the Cisco IOS Software Security Advisory bundled publication. Cisco recommends upgrading to the latest available release, where possible.

Major Release	Availability of Repaired Releases
Affected 12.0-Based Releases	First Fixed Release for All Advisories in the September 2010 Bundle Publication
There are no affected 12.0 based releases	
Affected 12.1-Based Releases	First Fixed Release for All Advisories in the September 2010 Bundle Publication
12.1	Vulnerable; first fixed in 12.4T Releases up to and including 12.1(4b) are not vulnerable.
12.1AA	Not Vulnerable
12.1AX	Not Vulnerable
12.1AY	Not Vulnerable
12.1AZ	Not Vulnerable
12.1CX	Not Vulnerable
12.1DA	Not Vulnerable
12.1DB	Not Vulnerable
12.1DC	Not Vulnerable
12.1E	Not Vulnerable
12.1EA	Not Vulnerable
12.1EB	Not Vulnerable
12.1EC	Not Vulnerable
12.1EO	Not Vulnerable
12.1EU	Not Vulnerable
12.1EV	Not Vulnerable
12.1EW	Not Vulnerable
12.1EX	Not Vulnerable
12.1EY	Not Vulnerable

12.1EZ	Not Vulnerable
12.1GA	Not Vulnerable
12.1GB	Not Vulnerable
12.1T	Vulnerable; first fixed in 12.4T Releases up to and including 12.1(3a)T8 are not vulnerable.
12.1XA	Not Vulnerable
12.1XB	Not Vulnerable
12.1XC	Not Vulnerable
12.1XD	Not Vulnerable
12.1XE	Not Vulnerable
12.1XF	Not Vulnerable
12.1XG	Not Vulnerable
12.1XH	Not Vulnerable
12.1XI	Vulnerable; first fixed in 12.4T
12.1XJ	Vulnerable; first fixed in 12.4T
12.1XL	Vulnerable; first fixed in 12.4T
12.1XM	Vulnerable; first fixed in 12.4T
12.1XP	Vulnerable; first fixed in 12.4T
12.1XQ	Vulnerable; first fixed in 12.4T
12.1XR	Vulnerable; first fixed in 12.4T
12.1XS	Vulnerable; first fixed in 12.4T Releases up to and including 12.1(3)XS are not vulnerable.
12.1XT	Vulnerable; first fixed in 12.4T Releases up to and including 12.1(2)XT2 are not vulnerable.
12.1XU	Vulnerable; first fixed in 12.4T

12.1XV	Vulnerable; first fixed in 12.4T
12.1XW	Not Vulnerable
12.1XX	Not Vulnerable
12.1XY	Vulnerable; first fixed in 12.4T Releases up to and including 12.1(4)XY are not vulnerable.
12.1XZ	Not Vulnerable
12.1YA	Vulnerable; first fixed in 12.4T
12.1YB	Vulnerable; first fixed in 12.4T
12.1YC	Vulnerable; first fixed in 12.4T
12.1YD	Vulnerable; first fixed in 12.4T
12.1YE	Releases prior to 12.1(5)YE6 are vulnerable, release 12.1(5)YE6 and later are not vulnerable; first fixed in 12.4T
12.1YF	Vulnerable; first fixed in 12.4T
12.1YH	Vulnerable; first fixed in 12.4T
12.1YI	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.1YJ	Not Vulnerable
Affected 12.2-Based Releases	First Fixed Release
12.2	Vulnerable; first fixed in 12.4T
12.2B	Vulnerable; first fixed in 12.4T Releases up to and including 12.2(2)B7 are not vulnerable.
12.2BC	Not Vulnerable
12.2BW	Vulnerable; first fixed in 12.4T
12.2BX	Vulnerable; first fixed in 12.2SB Releases up to and including 12.2(15)BX are not vulnerable.
12.2BY	Vulnerable; first fixed in 12.4T

	Releases up to and including 12.2(2)BY3 are not vulnerable.
12.2BZ	Not Vulnerable
12.2CX	Not Vulnerable
12.2CY	Not Vulnerable
12.2CZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2DA	Not Vulnerable
12.2DD	Vulnerable; first fixed in 12.4T
12.2DX	Vulnerable; first fixed in 12.4T
12.2EW	Not Vulnerable
12.2EWA	Not Vulnerable
12.2EX	Not Vulnerable
12.2EY	Not Vulnerable
12.2EZ	Not Vulnerable
12.2FX	Not Vulnerable
12.2FY	Not Vulnerable
12.2FZ	Not Vulnerable
12.2IRA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IRB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IRC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IRD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IRE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory

12.2IXB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXG	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2IXH	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2JA	Not Vulnerable
12.2JK	Not Vulnerable
12.2MB	Not Vulnerable
12.2MC	Releases up to and including 12.2(15)MC1 are not vulnerable. Releases 12.2(15)MC2b and later are not vulnerable; first fixed in 12.4T
12.2MRA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2MRB	12.2(33)MRB2
12.2S	Releases prior to 12.2(30)S are vulnerable, release 12.2(30)S and later are not vulnerable
12.2SB	12.2(31)SB19 Releases prior to 12.2(33)SB5 are vulnerable, release 12.2(33)SB5 and later are not vulnerable
12.2SBC	Vulnerable; first fixed in 12.2SB
12.2SCA	Vulnerable; first fixed in 12.2SCB
12.2SCB	12.2(33)SCB9
12.2SCC	12.2(33)SCC5
12.2SCD	12.2(33)SCD3

12.2SE	Not Vulnerable
12.2SEA	Not Vulnerable
12.2SEB	Not Vulnerable
12.2SEC	Not Vulnerable
12.2SED	Not Vulnerable
12.2SEE	Not Vulnerable
12.2SEF	Not Vulnerable
12.2SEG	Not Vulnerable
12.2SG	Releases prior to 12.2(40)SG are vulnerable, release 12.2(40)SG and later are not vulnerable; migrate to any release in 12.2SGA
12.2SGA	Not Vulnerable
12.2SL	Not Vulnerable
12.2SM	Not Vulnerable
12.2SO	Not Vulnerable
12.2SQ	Not Vulnerable
12.2SRA	Releases prior to 12.2(33)SRA6 are vulnerable, release 12.2(33)SRA6 and later are not vulnerable
12.2SRB	Releases prior to 12.2(33)SRB1 are vulnerable, release 12.2(33)SRB1 and later are not vulnerable
12.2SRC	Not Vulnerable
12.2SRD	Not Vulnerable
12.2SRE	12.2(33)SRE1
12.2STE	Not Vulnerable
12.2SU	Vulnerable; first fixed in 12.4T
12.2SV	Releases prior to 12.2(29b)SV1 are vulnerable, release 12.2(29b)SV1 and later are not vulnerable; migrate to any release in 12.2SVD
12.2SVA	Not Vulnerable

12.2SVC	Not Vulnerable
12.2SVD	Not Vulnerable
12.2SVE	Not Vulnerable
12.2SW	Releases up to and including 12.2(21)SW1 are not vulnerable. Releases 12.2(25)SW12 and later are not vulnerable; first fixed in 12.4T
12.2SX	Releases up to and including 12.2(14)SX2 are not vulnerable.
12.2SXA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2SXB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2SXD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2SXE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2SXF	Releases prior to 12.2(18)SXF11 are vulnerable, release 12.2(18)SXF11 and later are not vulnerable
12.2SXH	Not Vulnerable
12.2SXI	Not Vulnerable
12.2SY	Not Vulnerable
12.2SZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2T	Vulnerable; first fixed in 12.4T
12.2TPC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2XA	Vulnerable; first fixed in 12.4T
12.2XB	Vulnerable; first fixed in 12.4T
12.2XC	Vulnerable; first fixed in 12.4T
12.2XD	Vulnerable; first fixed in 12.4T
12.2XE	Not Vulnerable
12.2XF	Not Vulnerable

12.2XG	Vulnerable; first fixed in 12.4T
12.2XH	Vulnerable; first fixed in 12.4T
12.2XI	Vulnerable; first fixed in 12.4T
12.2XJ	Vulnerable; first fixed in 12.4T
12.2XK	Vulnerable; first fixed in 12.4T
12.2XL	Vulnerable; first fixed in 12.4T
12.2XM	Vulnerable; first fixed in 12.4T
12.2XN	Vulnerable; first fixed in 12.2SB
12.2XNA	Please see Cisco IOS-XE Software Availability
12.2XNB	Please see Cisco IOS-XE Software Availability
12.2XNC	Please see Cisco IOS-XE Software Availability
12.2XND	Please see Cisco IOS-XE Software Availability
12.2XNE	Please see Cisco IOS-XE Software Availability
12.2XNF	Please see Cisco IOS-XE Software Availability
12.2XO	Not Vulnerable
12.2XQ	Vulnerable; first fixed in 12.4T
12.2XR	Not Vulnerable
12.2XS	Vulnerable; first fixed in 12.4T
12.2XT	Vulnerable; first fixed in 12.4T
12.2XU	Vulnerable; first fixed in 12.4T
12.2XV	Vulnerable; first fixed in 12.4T
12.2XW	Vulnerable; first fixed in 12.4T
12.2YA	Vulnerable; first fixed in 12.4T

12.2YB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YG	Not Vulnerable
12.2YH	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YJ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YK	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YM	Vulnerable; first fixed in 12.4T
12.2YN	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YO	Not Vulnerable
12.2YP	Not Vulnerable
12.2YQ	Not Vulnerable
12.2YR	Not Vulnerable
12.2YS	Not Vulnerable
12.2YT	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YU	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YV	Releases prior to 12.2(11)YV1 are vulnerable, release 12.2(11)YV1 and later are not vulnerable

12.2YW	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YY	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZA	Not Vulnerable
12.2ZB	Releases up to and including 12.2(8)ZB are not vulnerable.
12.2ZC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZE	Vulnerable; first fixed in 12.4T
12.2ZF	Vulnerable; first fixed in 12.4T
12.2ZG	Not Vulnerable
12.2ZH	Vulnerable; first fixed in 12.4T
12.2ZI	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZP	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZU	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZX	Not Vulnerable
12.2ZY	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.2ZYA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
Affected 12.3-Based Releases	First Fixed Release

12.3	Vulnerable; first fixed in 12.4T
12.3B	Vulnerable; first fixed in 12.4T
12.3BC	Not Vulnerable
12.3BW	Not Vulnerable
12.3EU	Not Vulnerable
12.3JA	Not Vulnerable
12.3JEA	Not Vulnerable
12.3JEB	Not Vulnerable
12.3JEC	Not Vulnerable
12.3JED	Not Vulnerable
12.3JK	Releases up to and including 12.3(2)JK3 are not vulnerable. Releases 12.3(8)JK1 and later are not vulnerable; first fixed in 12.4T
12.3JL	Not Vulnerable
12.3JX	Not Vulnerable
12.3T	Vulnerable; first fixed in 12.4T
12.3TPC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3VA	Vulnerable; first fixed in 12.4T
12.3XA	Vulnerable; first fixed in 12.4T
12.3XB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3XC	Vulnerable; first fixed in 12.4T
12.3XD	Vulnerable; first fixed in 12.4T
12.3XE	Vulnerable; first fixed in 12.4T
12.3XF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory

12.3XG	Vulnerable; first fixed in 12.4T
12.3XI	Releases prior to 12.3(7)XI11 are vulnerable, release 12.3(7)XI11 and later are not vulnerable; first fixed in 12.2SB
12.3XJ	Vulnerable; first fixed in 12.4XR
12.3XK	Vulnerable; first fixed in 12.4T
12.3XL	Vulnerable; first fixed in 12.4T
12.3XQ	Vulnerable; first fixed in 12.4T
12.3XR	Vulnerable; first fixed in 12.4T
12.3XS	Vulnerable; first fixed in 12.4T
12.3XU	Vulnerable; first fixed in 12.4T
12.3XW	Vulnerable; first fixed in 12.4T
12.3XX	Vulnerable; first fixed in 12.4T
12.3XY	Vulnerable; first fixed in 12.4T
12.3XZ	Vulnerable; first fixed in 12.4T
12.3YA	Vulnerable; first fixed in 12.4T
12.3YD	Vulnerable; first fixed in 12.4T
12.3YF	Vulnerable; first fixed in 12.4XR
12.3YG	Vulnerable; first fixed in 12.4T
12.3YH	Vulnerable; first fixed in 12.4T
12.3YI	Vulnerable; first fixed in 12.4T
12.3YJ	Vulnerable; first fixed in 12.4T
12.3YK	Vulnerable; first fixed in 12.4T
12.3YM	Vulnerable; first fixed in 12.4T
12.3YQ	Vulnerable; first fixed in 12.4T
12.3YS	Vulnerable; first fixed in 12.4T

12.3YT	Vulnerable; first fixed in 12.4T
12.3YU	Vulnerable; first fixed in 12.4T
12.3YX	Vulnerable; first fixed in 12.4XR
12.3YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.3ZA	Vulnerable; first fixed in 12.4T
Affected 12.4-Based Releases	First Fixed Release
12.4	12.4(25d)
12.4GC	12.4(24)GC2
12.4JA	Not Vulnerable
12.4JDA	Not Vulnerable
12.4JDC	Not Vulnerable
12.4JDD	Not Vulnerable
12.4JHA	Not Vulnerable
12.4JHB	Not Vulnerable
12.4JK	Not Vulnerable
12.4JL	Not Vulnerable
12.4JMA	Not Vulnerable
12.4JMB	Not Vulnerable
12.4JX	Not Vulnerable
12.4JY	Not Vulnerable
12.4MD	12.4(24)MD2
12.4MDA	12.4(22)MDA4 12.4(24)MDA1

12.4MR	Vulnerable; first fixed in 12.4MRA
12.4MRA	12.4(20)MRA1
12.4SW	Vulnerable; first fixed in 12.4T
12.4T	12.4(15)T14 12.4(20)T6 12.4(24)T4
12.4XA	Vulnerable; first fixed in 12.4T
12.4XB	Vulnerable; first fixed in 12.4T
12.4XC	Vulnerable; first fixed in 12.4T
12.4XD	Vulnerable; first fixed in 12.4T
12.4XE	Releases prior to 12.4(6)XE5 are vulnerable, release 12.4(6)XE5 and later are not vulnerable; first fixed in 12.4T
12.4XF	Vulnerable; first fixed in 12.4T
12.4XG	Vulnerable; first fixed in 12.4T
12.4XJ	Vulnerable; first fixed in 12.4T
12.4XK	Vulnerable; first fixed in 12.4T
12.4XL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4XM	Vulnerable; first fixed in 12.4T
12.4XN	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4XP	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4XQ	12.4(15)XQ6; Available on 22-SEP-10
12.4XR	12.4(15)XR9 12.4(22)XR7
12.4XT	Vulnerable; first fixed in 12.4T
12.4XV	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory

12.4XW	Vulnerable; first fixed in 12.4T
12.4XY	Vulnerable; first fixed in 12.4T
12.4XZ	Vulnerable; first fixed in 12.4T
12.4YA	Vulnerable; first fixed in 12.4T
12.4YB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4YD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4YE	12.4(24)YE1
12.4YG	12.4(24)YG3
Affected 15.0-Based Releases	First Fixed Release
15.0M	15.0(1)M3
15.0S	Cisco 7600 and 10000 Series routers: 15.0(1)S1 (available early October 2010) Please see Cisco IOS-XE Software Availability
15.0XA	Vulnerable; first fixed in 15.1T
15.0XO	Not Vulnerable
Affected 15.1-Based Releases	First Fixed Release
15.1T	15.1(2)T1
15.1XB	Vulnerable; first fixed in 15.1T

Cisco IOS XE Software

Cisco IOS XE Release	First Fixed Release for All Advisories in the September 2010 Bundle Publication
2.1.x	Not Vulnerable
2.2.x	Not Vulnerable
2.3.x	Not Vulnerable
2.4.x	Not Vulnerable

2.5.x	Vulnerable; migrate to 2.6.2 or later
2.6.x	2.6.2
3.1.xS	Not Vulnerable

Cisco IOS XR System Software

Cisco IOS XR Software is not affected by the vulnerabilities disclosed in the September 22, 2010, Cisco IOS Software Security Advisory bundled publication.

[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](#)

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-20100922-bundle.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 1.0	2010-September-22	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)

□

Send

[Home](#) | [How to Buy](#) | [Login](#) | [Profile](#) | [Feedback](#) | [Site Map](#) | [Help](#)

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

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