

# Summary of Cisco IOS Software Bundled Advisories, March 24, 2010

Advisory ID: **cisco-sa-20100324-bundle**

<http://www.cisco.com/warp/public/707/cisco-sa-20100324-bundle.shtml>

## Revision 1.1

Last Updated 2010 March 25 1930 UTC (GMT)

For Public Release 2010 March 24 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 March 24, 2010, Cisco IOS<sup>®</sup> Software Security Advisory bundled publication includes seven Security Advisories. All the advisories address vulnerabilities in Cisco IOS Software. 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 March 24, 2010, or earlier.

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

[http://www.cisco.com/web/about/security/intelligence/Cisco\\_ERP\\_mar10.html](http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar10.html)

This list also includes all individual publication links:

- Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml>

- Cisco IOS Software Crafted TCP Packet Denial of Service Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-tcp.shtml>
- Cisco IOS Software IPsec Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-ipsec.shtml>
- Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities  
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-sip.shtml>
- Cisco IOS Software H.323 Denial of Service Vulnerabilities  
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml>
- Cisco IOS Software NAT Skinny Call Control Protocol Vulnerability  
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-sccp.shtml>
- Cisco Unified Communications Manager Express Denial of Service Vulnerabilities  
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-cucme.shtml>

This summary page is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100324-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 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 for this Advisory" column of the table. The "First Fixed Release for all Advisories in 24 March 2010 Bundle Publication" column indicates the earliest possible releases which have fixes for all the published vulnerabilities in this Cisco IOS 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 24 March 2010 Bundle Publication
12.0	Not Vulnerable

12.0DA	Not Vulnerable
12.0DB	Not Vulnerable
12.0DC	Not Vulnerable
12.0S	12.0(32)S15; Available on 25-MAR-10 12.0(33)S6
12.0SC	Not Vulnerable
12.0SL	Releases up to and including 12.0(14)SL1 are not vulnerable; First fixed in 12.0S
12.0SP	Not Vulnerable
12.0ST	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.0SX	Vulnerable; first fixed in <a href="#">12.0S</a>
12.0SY	12.0(32)SY11 12.0(32)SY9b
12.0SZ	Vulnerable; first fixed in <a href="#">12.0S</a>
12.0T	Not Vulnerable

12.0W	Not Vulnerable
12.0WC	Not Vulnerable
12.0WT	Not Vulnerable
12.0XA	Not Vulnerable
12.0XB	Not Vulnerable
12.0XC	Not Vulnerable
12.0XD	Not Vulnerable
12.0XE	Not Vulnerable
12.0XF	Not Vulnerable
12.0XG	Not Vulnerable
12.0XH	Not Vulnerable
12.0XI	Not Vulnerable

12.0XJ	Not Vulnerable
12.0XK	Not Vulnerable
12.0XL	Not Vulnerable
12.0XM	Not Vulnerable
12.0XN	Not Vulnerable
12.0XQ	Not Vulnerable
12.0XR	Not Vulnerable
12.0XS	Not Vulnerable
12.0XT	Not Vulnerable
12.0XV	Not Vulnerable
<b>Affected 12.1-Based Releases</b>	<b>First Fixed Release for all Advisories in 24 March 2010 Bundle Publication</b>
12.1	Not Vulnerable
12.1AA	Not Vulnerable

12.1AX	Releases up to and including 12.1(11)AX are not vulnerable; first fixed in 12.2SE
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	Releases up to and including 12.1(7a)E1a are not vulnerable; migrate to any release in 12.2SXF
12.1EA	Releases up to and including 12.1(6)EA2c are not vulnerable. Releases 12.1(8)EA1c and later are not vulnerable.
12.1EB	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.1EC	Releases up to and including 12.1(7)EC are not vulnerable; migrate to 12.2SCB
12.1EO	Releases up to and including 12.1(19)EO6 are not vulnerable.

12.1EU	Not Vulnerable
12.1EV	Not Vulnerable
12.1EW	Not Vulnerable
12.1EX	Vulnerable; migrate to any release in 12.2
12.1EY	Releases up to and including 12.1(7a)EY3 are not vulnerable.
12.1EZ	Not Vulnerable
12.1GA	Not Vulnerable
12.1GB	Not Vulnerable
12.1T	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	Not Vulnerable
12.1XJ	Not Vulnerable
12.1XL	Not Vulnerable
12.1XM	Not Vulnerable
12.1XP	Not Vulnerable
12.1XQ	Not Vulnerable
12.1XR	Not Vulnerable
12.1XS	Not Vulnerable

12.1XT	Not Vulnerable
12.1XU	Vulnerable; migrate to any release in 12.2
12.1XV	Releases prior to 12.1(5)XV1 are vulnerable, release 12.1(5)XV1 and later are not vulnerable
12.1XW	Not Vulnerable
12.1XX	Not Vulnerable
12.1XY	Not Vulnerable
12.1XZ	Not Vulnerable
12.1YA	Not Vulnerable
12.1YB	Vulnerable; migrate to any release in 12.2
12.1YC	Not Vulnerable
12.1YD	Vulnerable; migrate to any release in 12.2
12.1YE	Releases prior to 12.1(5)YE6 are vulnerable, release 12.1(5)YE6 and later are not vulnerable.
12.1YF	

	Not Vulnerable
12.1YH	Not Vulnerable
12.1YI	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.1YJ	Not Vulnerable
<b>Affected 12.2-Based Releases</b>	<b>First Fixed Release for all Advisories in 24 March 2010 Bundle Publication</b>
12.2	Not Vulnerable
12.2B	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BC	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BW	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BX	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BY	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2BZ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2CX	Vulnerable; migrate to any release in 15.0M or a

	fixed 12.4 release.
12.2CY	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2CZ	Vulnerable; migrate to any release in 12.2SRE
12.2DA	Not Vulnerable
12.2DD	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2DX	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2EW	Not Vulnerable
12.2EWA	Not Vulnerable
12.2EX	Releases up to and including 12.2(37)EX are not vulnerable.  Releases 12.2(44)EX and later are not vulnerable; first fixed in <a href="#">12.2SE</a>
12.2EY	Releases prior to 12.2(37)EY are vulnerable, release 12.2(37)EY and later are not vulnerable
12.2EZ	Not Vulnerable
12.2FX	Not Vulnerable

12.2FY	Not Vulnerable
12.2FZ	Not Vulnerable
12.2IRA	Vulnerable; first fixed in <a href="#">12.2SRC</a>
12.2IRB	Vulnerable; first fixed in <a href="#">12.2SRC</a>
12.2IRC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2IRD	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2IXA	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2IXB	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2IXC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2IXD	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2IXE	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory

12.2IXF	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2IXG	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2IXH	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2JA	Releases up to and including 12.2(4)JA1 are not vulnerable.
12.2JK	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2MB	Not Vulnerable
12.2MC	Vulnerable; first fixed in 12.4
12.2MRA	Not Vulnerable
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(33)SB8 12.2(31)SB18; Available on 24-MAR-10
12.2SBC	Vulnerable; migrate to any release in 12.2SRE
12.2SCA	Vulnerable; first fixed in <a href="#">12.2SCB</a>

12.2SCB	12.2(33)SCB6
12.2SCC	12.2(33)SCC1
12.2SCD	Not Vulnerable
12.2SE	12.2(50)SE4; Available on 25-MAR-10
12.2SEA	Not Vulnerable
12.2SEB	Not Vulnerable
12.2SEC	Not Vulnerable
12.2SED	Vulnerable; first fixed in <a href="#">12.2SE</a>
12.2SEE	Vulnerable; first fixed in <a href="#">12.2SE</a>
12.2SEF	Not Vulnerable
12.2SEG	Releases prior to 12.2(25)SEG4 are vulnerable, release 12.2(25)SEG4 and later are not vulnerable; first fixed in <a href="#">12.2SE</a>
12.2SG	Releases up to 12.2(31)SG1 are not vulnerable; releases 12.2(40)SG and later are not vulnerable.

12.2SGA	Not Vulnerable
12.2SL	Not Vulnerable
12.2SM	Not Vulnerable
12.2SO	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2SQ	Not Vulnerable
12.2SRA	Vulnerable; first fixed in <a href="#">12.2SRD</a>
12.2SRB	Vulnerable; first fixed in <a href="#">12.2SRD</a>
12.2SRC	12.2(33)SRC5
12.2SRD	12.2(33)SRD3
12.2SRE	Not Vulnerable
12.2STE	Not Vulnerable
12.2SU	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2SV	Releases up to and including 12.2(18)SV2 are not

	vulnerable.
12.2SVA	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2SVC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2SVD	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2SVE	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2SW	Releases up to and including 12.2(25)SW3 are not vulnerable.  Releases 12.2(25)SW12 and later are not vulnerable; first fixed in <a href="#">15.0M</a>
12.2SX	Vulnerable; first fixed in <a href="#">12.2SXF</a>
12.2SXA	Vulnerable; first fixed in <a href="#">12.2SXF</a>
12.2SXB	Vulnerable; first fixed in <a href="#">12.2SXF</a>
12.2SXD	Vulnerable; first fixed in <a href="#">12.2SXF</a>
12.2SXE	Vulnerable; first fixed in <a href="#">12.2SXF</a>
12.2SXF	

	12.2(18)SXF17a
12.2SXH	12.2(33)SXH6
12.2SXI	12.2(33)SXI2a 12.2(33)SXI3
12.2SY	Vulnerable; migrate to any release in 12.2SRE
12.2SZ	Vulnerable; migrate to any release in 12.2SRE
12.2T	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2TPC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2XA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XB	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XC	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XD	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XE	Not Vulnerable
12.2XF	Vulnerable; migrate to any release in 15.0M or a

	fixed 12.4 release.
12.2XG	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XH	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XI	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XJ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XK	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XL	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XM	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XN	Releases prior to 12.2(33)XN1 are vulnerable, release 12.2(33)XN1 and later are not vulnerable; first fixed in <a href="#">12.2SRC</a>
12.2XNA	Please see <a href="#">Cisco IOS-XE Software Availability</a>
12.2XNB	Please see <a href="#">Cisco IOS-XE Software Availability</a>
12.2XNC	Please see <a href="#">Cisco IOS-XE Software Availability</a>
12.2XND	Please see <a href="#">Cisco IOS-XE Software Availability</a>

12.2XNE	Please see <a href="#">Cisco IOS-XE Software Availability</a>
12.2XNF	Please see <a href="#">Cisco IOS-XE Software Availability</a>
12.2XO	Not Vulnerable
12.2XQ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XR	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XS	Not Vulnerable
12.2XT	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XU	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XV	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2XW	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2YA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2YB	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory

12.2YC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YD	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YE	Not Vulnerable
12.2YF	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YG	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YH	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YJ	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YK	Not Vulnerable
12.2YL	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YM	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2YN	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory

12.2YO	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YP	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2YQ	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YR	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YS	Not Vulnerable
12.2YT	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YU	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YV	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YW	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YX	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2YY	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section

	of this advisory
12.2YZ	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2ZA	Vulnerable; first fixed in <a href="#">12.2SXF</a>
12.2ZB	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2ZC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2ZD	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2ZE	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2ZF	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2ZG	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2ZH	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.2ZJ	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2ZL	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory

12.2ZP	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2ZU	Vulnerable; first fixed in <a href="#">12.2SXH</a>
12.2ZX	Vulnerable; migrate to any release in 12.2SRE
12.2ZY	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.2ZYA	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release for all Advisories in 24 March 2010 Bundle Publication</b>
12.3	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3B	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3BC	Vulnerable; first fixed in <a href="#">12.2SCB</a>
12.3BW	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3EU	Not Vulnerable

12.3JA	Releases prior to 12.3(11)JA5 are vulnerable, release 12.3(11)JA5 and later are not vulnerable
12.3JEA	Releases prior to 12.3(8)JEA4 are vulnerable, release 12.3(8)JEA4 and later are not vulnerable
12.3JEB	Releases prior to 12.3(8)JEB2 are vulnerable, release 12.3(8)JEB2 and later are not vulnerable
12.3JEC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.3JED	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.3JK	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3JL	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.3JX	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.3T	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3TPC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.3VA	Not Vulnerable
12.3XA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.3XB	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.3XC	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XD	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XE	Vulnerable; first fixed in <a href="#">12.4</a> Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XF	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.3XG	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XI	Releases prior to 12.3(7)XI11 are vulnerable, release 12.3(7)XI11 and later are not vulnerable
12.3XJ	Vulnerable; first fixed in <a href="#">12.4XR</a>
12.3XK	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XL	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XQ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.3XR	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XS	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XU	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XW	Vulnerable; first fixed in <a href="#">12.4XR</a>
12.3XX	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XY	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3XZ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YD	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YF	Vulnerable; first fixed in <a href="#">12.4XR</a>
12.3YG	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YH	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YI	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.3YJ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YK	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YM	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YQ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YS	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YT	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YU	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.3YX	Vulnerable; first fixed in <a href="#">12.4XR</a>
12.3YZ	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.3ZA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
<b>Affected 12.4-Based Releases</b>	<b>First Fixed Release for all Advisories in 24 March 2010 Bundle Publication</b>
12.4	12.4(25c) 15.0(1)M1

12.4GC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4JA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory
12.4JDA	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4JDC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4JDD	12.4(10b)JDD1
12.4JHA	Not Vulnerable
12.4JK	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4JL	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4JMA	Releases prior to 12.4(3g)JMA2 are vulnerable, release 12.4(3g)JMA2 and later are not vulnerable
12.4JMB	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4JX	Vulnerable; first fixed in <a href="#">12.4JA</a>

12.4MD	12.4(24)MD
12.4MDA	12.4(22)MDA2
12.4MR	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4SW	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4T	12.4(15)T12 12.4(20)T5 12.4(24)T3; Available on 26-MAR-10 12.4(22)T4
12.4XA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XB	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XC	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XD	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XE	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XF	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.4XG	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XJ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XK	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XL	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4XM	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XN	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4XP	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4XQ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XR	12.4(22)XR3
12.4XT	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XV	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4XW	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.

12.4XY	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4XZ	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4YA	Vulnerable; migrate to any release in 15.0M or a fixed 12.4 release.
12.4YB	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4YD	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
12.4YE	12.4(22)YE2 12.4(24)YE
12.4YG	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory
<b>Affected 15.0-Based Releases</b>	<b>First Fixed Release for all Advisories in 24 March 2010 Bundle Publication</b>
15.0M	15.0(1)M1
<b>Affected 15.1-Based Releases</b>	<b>First Fixed Release for all Advisories in 24 March 2010 Bundle Publication</b>
There are no affected 15.1 based releases	

## Cisco IOS-XE Software

IOS-XE Release	First Fixed Release
2.1.x	Vulnerable, Migrate to 2.5.1 or later
2.2.x	Vulnerable, Migrate to 2.5.1 or later
2.3.x	2.3.2
2.4.x	Not Vulnerable
2.5.x	2.5.1
2.6.x	Not Vulnerable

## Cisco IOS XR System Software

These vulnerabilities can be addressed by applying the appropriate Software Maintenance Upgrade (SMU), per the table below. Installation of the appropriate SMU does not require a system reload. Refer to the document "Guidelines for Cisco IOS XR Software" at the following link for additional information on Cisco IOS XR Software and SMUs: [http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8803/ps5845/product\\_bulletin\\_c25-478699.htm](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8803/ps5845/product_bulletin_c25-478699.htm)

Cisco IOS XR Software Version	SMU ID	SMU Name
3.2.X	Vulnerable; Migrate to 3.5.2 or later.	
3.3.X	Vulnerable; Migrate to 3.5.2 or later.	
3.4.0	Vulnerable; Migrate to 3.5.2 or later.	

3.4.1	AA03710 AA03707	c12k-mpls- 3.4.1.CSCsj25893  hfr-mpls- 3.4.1.CSCsj25893
3.4.2	AA03711 AA03708	c12k-mpls- 3.4.2.CSCsj25893  hfr-mpls- 3.4.2.CSCsj25893
3.4.3	AA03712 AA03709	c12k-mpls- 3.4.3.CSCsj25893  hfr-mpls- 3.4.3.CSCsj25893
3.5.2	Not Vulnerable	
3.5.3	Not Vulnerable	
3.5.4	Not Vulnerable	
3.6.X	Not Vulnerable	
3.7.X	Not Vulnerable	
3.8.X	Not Vulnerable	
3.9.X	Not Vulnerable	

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

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto:security-alert@cisco.com) for software upgrades.

## ☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

## ☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

## ☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

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

## ☐ **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-20100324-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](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 1.1	2010-Mar-25	Made update to Cisco IOS-XE table.
Revision 1.0	2010-Mar-24	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.](#)