

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Security Advisories

Cisco Security Advisory: Combined IOS Table for May 22, 2007 Security Advisories

Advisory ID: [cisco-sa-20070522-cry-bundle.shtml](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>

Revision 1.1

Last Updated 2007 May 22 1515 UTC (GMT)

For Public Release 2007 May 22 1300 UTC (GMT)

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

Contents

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

Summary

On May 22 2007, Cisco released two security advisories. This document is provided for reference to customers who wish to upgrade to one version of Cisco IOS software that has all the fixes from the two advisories. The two advisories are available at:

- <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

To assist customers in their software migration strategies, a Software Versions and Fixes table is shown below that captures the first fixed release of Cisco IOS for the two advisories listed above.

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) describes a release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. 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. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.sht

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Release	Rebuild	Maintenance
12.0T	Vulnerable; migrate to 12.2(46) or later	
12.0WC	12.0(5)WC17	
12.0XE	Vulnerable; migrate to 12.1(26)E8 or later	
12.0XH	Vulnerable; migrate to 12.2(46) or later	
12.0XI	Vulnerable; migrate to 12.2(46) or later	
12.0XK	Vulnerable; migrate to 12.2(46) or later	
12.0XL	Vulnerable; migrate to 12.2(46) or later	
12.0XN	Vulnerable; migrate to 12.2(46) or later	
12.0XQ	Vulnerable; migrate to 12.2(46) or later	
12.0XR	Vulnerable; migrate to 12.2(46) or later	
12.0XV	Vulnerable; migrate to 12.2(46) or later	
Affected 12.1-Based	Rebuild	Maintenance

Release		
12.1	Vulnerable; migrate to 12.2(46) or later	
12.1AY	Vulnerable; migrate to 12.1(22)EA9 or later	
12.1CX	Vulnerable; migrate to 12.2(46) or later	
12.1E	12.1(26)E8	
	12.1(27b)E2; available 25-June-07	
12.1EA	12.1(22)EA9	
12.1EB	12.1(26)EB2; available 30-July-07	
12.1EC	Vulnerable; migrate to 12.3(21)BC or later	
12.1EW	Vulnerable; migrate to 12.2(25)EWA9 or later	
12.1EX	Vulnerable; migrate to 12.1(26)E8 or later	
12.1EY	Vulnerable; migrate to 12.1(26)E8 or later	
12.1T	Vulnerable; migrate to 12.2(46) or later	
12.1XC	Vulnerable; migrate to 12.2(46) or later	
12.1XD	Vulnerable; migrate to 12.2(46) or later	
12.1XF	Vulnerable; migrate 12.3(22) or later	
12.1XG	Vulnerable; migrate 12.3(22) or later	
12.1XH	Vulnerable; migrate to 12.2(46) or later	
12.1XI	Vulnerable; migrate to 12.2(46) or later	
12.1XJ	Vulnerable; migrate 12.3(22) or later	
12.1XL	Vulnerable; migrate 12.3(22) or later	
12.1XM	Vulnerable; migrate 12.3(22) or later	
12.1XP	Vulnerable; migrate 12.3(22) or later	
12.1XQ	Vulnerable; migrate 12.3(22) or later	
12.1XT	Vulnerable; migrate 12.3(22) or later	
12.1XU	Vulnerable; migrate 12.3(22) or later	
12.1YB	Vulnerable; migrate 12.3(22) or later	
12.1YC	Vulnerable; migrate 12.3(22) or later	
12.1YD	Vulnerable; migrate 12.3(22) or later	
12.1YE	Vulnerable; migrate 12.3(22) or later	
12.1YF	Vulnerable; migrate 12.3(22) or later	
12.1YI	Vulnerable; migrate 12.3(22) or later	

Affected 12.2- Based Release	Rebuild	Maintenance
12.2	12.2(40a)	12.2(46)
12.2B	Vulnerable; migrate to 12.4(10) or later	
12.2BC	Vulnerable; migrate to 12.3(21)BC or later	
12.2BW	Vulnerable; migrate 12.3(22) or later	
12.2BY	Vulnerable; migrate to 12.4(10) or later	
12.2BZ	Vulnerable; contact TAC	
12.2CX	Vulnerable; migrate to 12.3(21)BC or later	
12.2CY	Vulnerable; migrate to 12.3(21)BC or later	
12.2CZ	Vulnerable; contact TAC	
12.2DD	Vulnerable; migrate to 12.4(10) or later	
12.2EW	Vulnerable; migrate to 12.2(25)EWA9 or later	
12.2EWA	12.2(25)EWA9	
12.2EX	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2EY	Vulnerable; migrate to 12.2(35)SEE3 or later	
12.2EZ	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2FX	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2FY	Vulnerable; migrate to 12.2(35)SE2 or later	
12.2FZ	Vulnerable; migrate to 12.2(35)SE2 or later	
12.2JA	Vulnerable; contact TAC	
12.2JK	Vulnerable; migrate to 12.4(11)T1 or later	
12.2S		12.2(25)S12
12.2SB	12.2(31)SB2	
12.2SBC	Vulnerable; migrate to 12.2(31)SB2 or later	
12.2SE		12.2(35)SE
12.2SEA	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2SEB	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2SEC	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2SED	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2SEE	12.2(25)SEE3	
12.2SEF	Vulnerable; migrate to 12.2(35)SE2 or later	

12.2SEG	12.2(25)SEG2	
12.2SG		12.2(37)SG
12.2SGA	12.2(31)SGA1	
12.2SRA	12.2(33)SRA3	
12.2SRB		12.2(33)SRB
12.2SU	Vulnerable; migrate to 12.4(10) or later	
12.2SV	12.2(28)SV2	
	12.2(29)SV3	
12.2SW	12.2(25)SW9	
12.2SX	Vulnerable; migrate to 12.2(18)SXE6a or later	
12.2SXA	Vulnerable; migrate to 12.2(18)SXE6a or later	
12.2SXB	Vulnerable; migrate to 12.2(18)SXE6a or later	
12.2SXD	Vulnerable; migrate to 12.2(18)SXF8 or later	
12.2SXE	Vulnerable; migrate to 12.2(18)SXF8 or later	
12.2SXF	12.2(18)SXF8	
12.2SY	Vulnerable; migrate to 12.2(18)SXE6a or later	
12.2T	Vulnerable; migrate 12.3(22) or later	
12.2TPC	12.2(8)TPC10b	
12.2XA	Vulnerable; migrate 12.3(22) or later	
12.2XB	Vulnerable; migrate 12.3(22) or later	
12.2XD	Vulnerable; migrate 12.3(22) or later	
12.2XE	Vulnerable; migrate 12.3(22) or later	
12.2XF	Vulnerable; migrate to 12.3(21)BC or later	
12.2XG	Vulnerable; migrate 12.3(22) or later	
12.2XH	Vulnerable; migrate 12.3(22) or later	
12.2XI	Vulnerable; migrate 12.3(22) or later	
12.2XJ	Vulnerable; migrate 12.3(22) or later	
12.2 XK	Vulnerable; migrate 12.3(22) or later	
12.2XL	Vulnerable; migrate 12.3(22) or later	
12.2XM	Vulnerable; migrate 12.3(22) or later	
12.2XN	Vulnerable; migrate 12.3(22) or later	
12.2XQ	Vulnerable; migrate 12.3(22) or later	
12.2XR	Vulnerable; migrate 12.3(22) or later	
12.2XS	Vulnerable; migrate 12.3(22) or later	

12.2XT	Vulnerable; migrate 12.3(22) or later
12.2XU	Vulnerable; migrate 12.3(22) or later
12.2XV	Vulnerable; migrate 12.3(22) or later
12.2XW	Vulnerable; migrate 12.3(22) or later
12.2YA	Vulnerable; migrate 12.3(22) or later
12.2YB	Vulnerable; migrate 12.3(22) or later
12.2YC	Vulnerable; migrate 12.3(22) or later
12.2YD	Vulnerable; migrate to 12.4(10) or later
12.2YE	Vulnerable; migrate to 12.2(25)S12 or later
12.2YF	Vulnerable; migrate 12.3(22) or later
12.2YJ	Vulnerable; migrate 12.3(22) or later
12.2YL	Vulnerable; migrate to 12.4(10) or later
12.2YM	Vulnerable; migrate to 12.4(10) or later
12.2YN	Vulnerable; migrate to 12.4(10) or later
12.2YQ	Vulnerable; migrate to 12.4(10) or later
12.2YR	Vulnerable; migrate to 12.4(10) or later
12.2YU	Vulnerable; migrate to 12.4(10) or later
12.2YV	Vulnerable; migrate to 12.4(10) or later
12.2YW	Vulnerable; migrate to 12.4(10) or later
12.2YX	Vulnerable; migrate to 12.4(10) or later
12.2YY	Vulnerable; migrate to 12.4(10) or later
12.2YZ	Vulnerable; contact TAC
12.2ZA	Vulnerable; migrate to 12.2(18)SXE6a or later
12.2ZB	Vulnerable; migrate to 12.4(10) or later
12.2ZD	Vulnerable; contact TAC
12.2ZE	Vulnerable; migrate 12.3(22) or later
12.2ZF	Vulnerable; migrate to 12.4(10) or later
12.2ZG	Vulnerable; contact TAC
12.2ZH	Vulnerable; contact TAC
12.2ZJ	Vulnerable; migrate to 12.4(10) or later
12.2ZL	Vulnerable; contact TAC
12.2ZN	Vulnerable; migrate to 12.4(10) or later
12.2ZU	Vulnerable; contact TAC
12.2ZV	Vulnerable; contact TAC

12.2ZW	Vulnerable; contact TAC	
12.2ZX	Vulnerable; contact TAC	
Affected 12.3- Based Release	Rebuild	Maintenance
12.3	12.3(21a)	12.3(22)
12.3B	Vulnerable; migrate to 12.4(10) or later	
12.3BC		12.3(21)BC
12.3JA	Vulnerable; contact TAC	
12.3JEA	Vulnerable; contact TAC	
12.3JK	Vulnerable; contact TAC	
12.3JL	Vulnerable; contact TAC	
12.3JX	Vulnerable; contact TAC	
12.3T	Vulnerable; migrate to 12.4(10) or later	
12.3TPC	Vulnerable; contact TAC	
12.3XA	Vulnerable; contact TAC	
12.3XB	Vulnerable; migrate to 12.4(10) or later	
12.3XC	Vulnerable; contact TAC	
12.3XD	Vulnerable; migrate to 12.4(10) or later	
12.3XE	Vulnerable; contact TAC	
12.3XF	Vulnerable; migrate to 12.4(10) or later	
12.3XG	Vulnerable; contact TAC	
12.3XH	Vulnerable; migrate to 12.4(10) or later	
12.3XI	Vulnerable; contact TAC	
12.3XJ	Vulnerable; contact TAC	
12.3XK	Vulnerable; contact TAC	
12.3XQ	Vulnerable; migrate to 12.4(10) or later	
12.3XR	Vulnerable; contact TAC	
12.3XS	Vulnerable; migrate to 12.4(10) or later	
12.3XU	Vulnerable; migrate to 12.4(11)T1 or later	
12.3XW	Vulnerable; contact TAC	
12.3XX	12.3(8)XX2d	
12.3YA	Vulnerable; contact TAC	

12.3YD	Vulnerable; migrate to 12.4(11)T1 or later	
12.3YF	Vulnerable; contact TAC	
12.3YG	Vulnerable; migrate to 12.4(11)T1 or later	
12.3YH	Vulnerable; migrate to 12.4(11)T1 or later	
12.3YI	Vulnerable; migrate to 12.4(11)T1 or later	
12.3YK	Vulnerable; migrate to 12.4(11)T1 or later	
12.3YQ	Vulnerable; migrate to 12.4(11)T1 or later	
12.3YS	Vulnerable; migrate to 12.4(11)T1 or later	
12.3YT	Vulnerable; migrate to 12.4(11)T1 or later	
12.3YU	Vulnerable; contact TAC	
12.3YX	12.3(14)YX7	
12.3YZ	Vulnerable; contact TAC	
Affected 12.4- Based Release	Rebuild	Maintenance
12.4	12.4(7d)	12.4(10)
12.4SW	12.4(11)SW1	
12.4T	12.4(6)T7	
	12.4(11)T1	
12.4XA	Vulnerable; migrate to 12.4(11)T1 or later	
12.4XB	Vulnerable; contact TAC	
12.4XC	12.4(4)XC6	
12.4XD	12.4(4)XD6	
12.4XE	Vulnerable; contact TAC	
12.4XJ	12.4(11)XJ2	

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "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 agreement 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 who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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

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

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Status of This Notice: Interim

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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.

Distribution

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-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-teams@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.

Revision History

Revision 1.1	2007-May-25	Updated fixed IOS releases
Revision 1.0	2007-May-22	Initial public release.

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>.

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
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).