

Cisco Security Advisory: Cisco IOS Software Secure Copy Privilege Escalation Vulnerability

Advisory ID: cisco-sa-20090325-scp

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

Revision 1.3

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

The server side of the Secure Copy (SCP) implementation in Cisco IOS software

contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

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

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory.

Individual publication links are listed below:

- Cisco IOS cTCP Denial of Service Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>
- Cisco IOS Software Multiple Features IP Sockets Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>
- Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>
- Cisco IOS Software Secure Copy Privilege Escalation Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>

- Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml>
- Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml>
- Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>
- Cisco IOS Software WebVPN and SSLVPN Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

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

☐ Affected Products

☐ Vulnerable Products

Cisco devices running an affected Cisco IOS software release, configured to offer SCP server functionality, and configured to use role-based ACL access are affected by this issue.

A device running a vulnerable Cisco IOS software release is affected if its configuration is similar to the following:

```
parser view <view name>
  <Definition of the CLI view>
  !
username <user ID> view <view name> secret <some secret>
!
ip scp server enable
```

In the above configuration snippet, the **parser view** command defines a view that specifies what commands users in that view can execute. The **username** command defines a local user and attaches, via the **view** keyword, the previously defined view to the user. And finally, the **ip scp server enable** command enables the Cisco IOS SCP server.

The absence of the **username** command does not guarantee that the device's configuration is not affected by this vulnerability because the name of a CLI view can be supplied by means of an Authentication, Authorization, and Accounting (AAA) server by using the **cli-view-name** attribute.

Note: The CLI view attached to a user can be supplied by a AAA server. When inspecting a device's configuration to determine if it is affected by this vulnerability it is better to check if the SCP service is enabled (**ip scp server enabled** command) and whether there are any CLI views defined (**parser view** command).

The Cisco IOS SCP server and role-based CLI access features are disabled by default.

The SCP server functionality is only available on encryption-capable images. Encryption-capable images are those that contain either a "k8" or "k9" in the image name, for example, "C7200-ADVSECURITYK9-M". Devices that do not run encryption-capable images are not vulnerable. If a device is running an encryption-capable image, the presence in the configuration of the **ip scp server enable** command, the existence of CLI views (**parser view** command), and whether there are users (local or remote) attached to these views will determine if the device is affected.

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>.

Cisco IOS XE Software is also affected by this vulnerability.

▣ **Products Confirmed Not Vulnerable**

Cisco devices that do not run Cisco IOS software are not affected.

Cisco IOS devices that do not have the SCP server feature enabled, or that make use of the feature but do not have the role-based CLI feature enabled, are not affected.

Cisco IOS XR Software is not affected.

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

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

▣ **Details**

SCP is a protocol similar to the Remote Copy (RCP) protocol, which allows the transfer of files between systems. The main difference between SCP and RCP is that in SCP, all aspects of the file transfer session, including authentication, occur in encrypted form, which makes SCP a more secure alternative than RCP. SCP relies on the Secure Shell (SSH) protocol, which uses TCP port 22 by default.

The Role-Based CLI Access feature allows the network administrator to define "views". Views are sets of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS software EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. For more information about the Role-Based CLI Access feature, reference http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html.

The server side of the SCP implementation in Cisco IOS software contains a vulnerability that allows authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be a SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow authenticated users to retrieve or write to any file on the device's file system, including the device's saved

configuration and Cisco IOS image files. This configuration file may include passwords or other sensitive information.

In the affected configuration presented in the [Affected Products](#) section, users confined to a CLI view can elevate their privileges by using SCP to write to the device's configuration. Note that a view can be attached to a user when defining the user in the local database (via the **username <user name> view ...** command), or by passing the attribute **cli-view-name** from an AAA server.

This vulnerability does not allow for authentication bypass; login credentials are verified and access is only granted if a valid username and password is provided. This vulnerability may cause authorization to be bypassed.

This vulnerability is documented in the Cisco Bug ID [CSCsv38166](#) ([registered customers only](#)) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-0637.

[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>.

CSCsv38166 - SCP + views (role-based CLI) allows privilege escalation					
Calculate the environmental score of CSCsv38166					
CVSS Base Score - 9.0					
Access	Access	Authentication	Confidentiality	Integrity	Availability

Vector	Complexity		Impact	Impact	Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - 7.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

▣ Impact

Successful exploitation of the vulnerability described in this advisory may allow valid but unauthorized users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files. This configuration file may include passwords or other sensitive information.

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

▣ Software Versions and Fixes

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

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

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected		

12.0- Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases		
Affected 12.1- Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2- Based Releases	First Fixed Release	Recommended Release
12.2	Not Vulnerable	
12.2B	Not Vulnerable	
12.2BC	Not Vulnerable	
12.2BW	Not Vulnerable	
12.2BX	Not Vulnerable	
12.2BY	Not Vulnerable	
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Not Vulnerable	
12.2DA	Not Vulnerable	
12.2DD	Not Vulnerable	
12.2DX	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	
12.2EX	Vulnerable; migrate to any release in 12.2SEG	12.2(44)SE6
12.2EY	Vulnerable; first fixed in 12.2SE	12.2(44)SE6
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	

12.2FY	Not Vulnerable	
12.2FZ	Not Vulnerable	
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	Not Vulnerable	
12.2IXB	Not Vulnerable	
12.2IXC	Not Vulnerable	
12.2IXD	Not Vulnerable	
12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2IXG	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	
12.2S	Not Vulnerable	
12.2SB	12.2(33)SB4	12.2(33)SB4
12.2SBC	Not Vulnerable	
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(44)SE6
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	12.2(52)SG; Available on 15- MAY-2009	12.2(52)SG; Available on 15- MAY-2009
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SQ	Vulnerable; contact TAC	
12.2SRA	Not Vulnerable	
12.2SRB	Vulnerable; first fixed in 12.2SRC	12.2(33)SRC4; Available on 18- MAY-2009 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	12.2(33)SRD1	12.2(33)SRD1
12.2STE	Vulnerable; contact TAC	
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SVE	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Not Vulnerable	
12.2SXE	Not Vulnerable	

12.2SXF	Not Vulnerable	
12.2SXH	Not Vulnerable	
12.2SXI	12.2(33)SXI1	12.2(33)SXI1
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Not Vulnerable	
12.2TPC	Not Vulnerable	
12.2XA	Not Vulnerable	
12.2XB	Not Vulnerable	
12.2XC	Not Vulnerable	
12.2XD	Not Vulnerable	
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	
12.2XG	Not Vulnerable	
12.2XH	Not Vulnerable	
12.2XI	Not Vulnerable	
12.2XJ	Not Vulnerable	
12.2XK	Not Vulnerable	
12.2XL	Not Vulnerable	
12.2XM	Not Vulnerable	
12.2XN	Vulnerable; first fixed in 12.2SRC	12.2(33)SB4 12.2(33)SRD1 12.2(33)SRC4; Available on 18-MAY-2009
12.2XNA	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD1 12.2(33)SRC4; Available on 18-MAY-2009
12.2XNB	12.2(33)XNB3	12.2(33)XNB3
12.2XNC	Not Vulnerable	
12.2XO	Not Vulnerable	
12.2XQ	Not Vulnerable	

12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Not Vulnerable	
12.2XU	Not Vulnerable	
12.2XV	Not Vulnerable	
12.2XW	Not Vulnerable	
12.2YA	Not Vulnerable	
12.2YB	Not Vulnerable	
12.2YC	Not Vulnerable	
12.2YD	Not Vulnerable	
12.2YE	Not Vulnerable	
12.2YF	Not Vulnerable	
12.2YG	Not Vulnerable	
12.2YH	Not Vulnerable	
12.2YJ	Not Vulnerable	
12.2YK	Not Vulnerable	
12.2YL	Not Vulnerable	
12.2YM	Not Vulnerable	
12.2YN	Not Vulnerable	
12.2YO	Not Vulnerable	
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	
12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Not Vulnerable	
12.2YU	Not Vulnerable	
12.2YV	Not Vulnerable	
12.2YW	Not Vulnerable	
12.2YX	Not Vulnerable	
12.2YY	Not Vulnerable	
12.2YZ	Not Vulnerable	
12.2ZA	Not Vulnerable	

12.2ZB	Not Vulnerable	
12.2ZC	Not Vulnerable	
12.2ZD	Not Vulnerable	
12.2ZE	Not Vulnerable	
12.2ZF	Not Vulnerable	
12.2ZG	Not Vulnerable	
12.2ZH	Not Vulnerable	
12.2ZJ	Not Vulnerable	
12.2ZL	Not Vulnerable	
12.2ZP	Not Vulnerable	
12.2ZU	Not Vulnerable	
12.2ZX	Not Vulnerable	
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	
Affected 12.3- Based Releases	First Fixed Release	Recommended Release
12.3	Not Vulnerable	
12.3B	Not Vulnerable	
12.3BC	Not Vulnerable	
12.3BW	Not Vulnerable	
12.3EU	Not Vulnerable	
12.3JA	Vulnerable; contact TAC	
12.3JEA	Vulnerable; contact TAC	
12.3JEB	Vulnerable; contact TAC	
12.3JEC	Vulnerable; contact TAC	
12.3JK	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009

12.3JL	Not Vulnerable	
12.3JX	Vulnerable; contact TAC	
12.3T	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.3TPC	Not Vulnerable	
12.3VA	Vulnerable; contact TAC	
12.3XA	Not Vulnerable	
12.3XB	Not Vulnerable	
12.3XC	Not Vulnerable	
12.3XD	Not Vulnerable	
12.3XE	Not Vulnerable	
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	12.4(22)T1 12.4(15)T9;

	fixed in 12.4T	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	Not Vulnerable	
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
12.3YH	Vulnerable; first fixed in 12.4T	12.4(22)T1 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
		12.4(22)T1

12.3YU	Vulnerable; first fixed in 12.4T	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(23a); Available on 05-JUN-2009	12.4(18e) 12.4(23a); Available on 05-JUN-2009
12.4JA	Vulnerable; contact TAC	
12.4JDA	Vulnerable; contact TAC	
12.4JK	Vulnerable; contact TAC	
12.4JL	Vulnerable; contact TAC	
12.4JMA	Vulnerable; contact TAC	
12.4JMB	Vulnerable; contact TAC	
12.4JX	Vulnerable; contact TAC	
12.4MD	12.4(11)MD7	12.4(11)MD7
12.4MR	12.4(19)MR2	12.4(19)MR2
12.4SW	Vulnerable; contact TAC	
	12.4(24)T	

12.4T	12.4(20)T2 12.4(22)T1 12.4(15)T9; Available on 29- APR-2009	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XA	Vulnerable; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; Available on 29- APR-2009
12.4XB	Vulnerable; first fixed in 12.4T	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(20)T2 12.4(22)T1	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	Releases prior to 12.4(15)XL4 are vulnerable, release 12.4(15)XL4 and later are not vulnerable;	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	Vulnerable; first fixed in 12.4T	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 Cisco IOS SCP server functionality is not needed then the vulnerability described in this document can be mitigated by disabling the SCP server or the CLI view feature. The SCP server can be disabled by executing the following command in global configuration mode:

```
no ip scp server enable
```

If the SCP server cannot be disabled due to operational concerns, then no workarounds exist. The risk posed by this vulnerability can be mitigated by following the best practices detailed in "Cisco Guide to Harden Cisco IOS Devices" at

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080

Please refer to the Obtaining Fixed Software section of this advisory for appropriate solutions to resolve this vulnerability.

Due to the nature of this vulnerability, networking best practices like access control lists (ACLs) and Control Plane Policing (CoPP) that restrict access to a device to certain IP addresses or subnetworks may not be effective. If access is already granted to a specific IP address or subnetwork, a user with low privileges will be able to establish an SCP session with the device, which would allow the user to exploit this vulnerability.

[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 reported to Cisco by Kevin Graham. Cisco would like to thank Mr. Graham for reporting this vulnerability and working with us towards coordinated disclosure of the vulnerability.

[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-scp.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 1.3	2009- June-26	Removed references to the March/09 combined fixed software table.
Revision 1.2	2009- June-1	Updated expected public availability date for release 12.4(23a).
Revision 1.1	2009- May-1	Updated expected public availability date for release 12.4(23a).
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.](#)