

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

Cisco Security Advisory: Cisco IOS Secure Copy Authorization Bypass Vulnerability

Advisory ID: cisco-sa-20070808-scp

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml>

Revision 1.0

For Public Release 2007 August 08 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 Internetwork Operating System (IOS) contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS Secure Copy Server service are not affected by this vulnerability.

This vulnerability does not apply to the IOS Secure Copy Client feature.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml>.

Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The advisories all affect IOS, one additionally affects Cisco Unified Communications Manager as well. Each advisory lists the releases that correct the vulnerability described in the advisory, and the advisories also detail the releases that correct the vulnerabilities in all four advisories. Individual publication links are listed below:

- Cisco IOS Information Leakage Using IPv6 Routing Header
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml>
- Cisco IOS Next Hop Resolution Protocol Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml>
- Cisco IOS Secure Copy Authorization Bypass Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml>
- Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>
- Cisco Unified MeetingPlace XSS Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml>

Affected Products

Vulnerable Products

Cisco devices running *certain* 12.2-based IOS releases *and* configured to offer Secure Copy server functionality are affected by this issue.

A device running a vulnerable Cisco IOS 12.2-based is affected if the following command is present in the device configuration:

```
ip scp server enable
```

The IOS Secure Copy server is disabled by default.

The Secure Copy server functionality is only available on encryption-capable images. Devices that do not run an encryption-capable images, which contain either k8 or k9 in the image name, are not vulnerable. If a device is running an encryption-capable image, the existence of the **ip scp server enable** command in the configuration will determine whether the device is affected.

Please consult the table of fixed software in the [Software Version and Fixes](#) section for the specific 12.2-based IOS releases that are affected.

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS". The image name will be displayed between parentheses

on the next line of output followed by "Version" and IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco product running IOS release 12.2(18)SXF10:

```
Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-IPSERVICESK9-M), Version 12.2(18)SXF10,
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by cisco Systems, Inc.
Compiled Fri 13-Jul-07 08:32 by kellythw
```

Additional information about Cisco IOS release naming is available at <http://www.cisco.com/warp/public/620/1.html>.

Products Confirmed Not Vulnerable

Cisco devices that do not run IOS are not affected.

Cisco IOS devices that do not have the Secure Copy server feature enabled are not affected.

The following IOS release trains are not affected:

- 12.0-based releases
- 12.1-based releases
- 12.3-based releases
- 12.4-based releases

Cisco IOS XR is not affected.

No other Cisco devices are known to be affected.

Details

Secure Copy (SCP) is a protocol similar to the Remote Copy (RCP) protocol, which allows for 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 server side of the Secure Copy implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

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.

A device with the Secure Copy server enabled is vulnerable regardless of whether Authentication,

Authorization, and Accounting (AAA) is enabled. If access control is enabled on the Virtual Terminal (vty) via the **login** command, which allows logins via Virtual Terminals, then the device is affected.

This vulnerability is documented in Cisco Bug ID [CSCsc19259](#) ([registered](#) customers only) .

Vulnerability Scoring Details

Cisco is providing 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 1.0.

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.


CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

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>.

CSCsc19259						
Calculate the environmental score of CSCsc19259 						
CVSS Base Score - 6.0						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - 5.0						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

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 filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

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.

For further information about how Cisco IOS is built, numbered and maintained, please see the following URL: <http://www.cisco.com/warp/public/620/1.html>

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Release	First Fixed Release	Recommended Release
There are no affected 12.0 based releases		
Affected 12.1-Based Release	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2-Based Release	First Fixed Release	Recommended Release
12.2	Not Vulnerable	
12.2B	Not Vulnerable	
12.2BC	Not Vulnerable	
12.2BW	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	
12.2EU	Not Vulnerable	
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	
12.2IXA	Vulnerable; first fixed in 12.2(18)IXD1	12.2(18)IXD1
12.2IXB	Vulnerable; first fixed in 12.2(18)IXD1	12.2(18)IXD1
12.2IXC	Vulnerable; first fixed in 12.2(18)IXD1	12.2(18)IXD1
12.2IXD	12.2(18)IXD1	12.2(18)IXD1
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	
12.2S	Not Vulnerable	
12.2SB	Not Vulnerable	
12.2SBC	Not Vulnerable	
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	Not Vulnerable	
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SRA	Not Vulnerable	
12.2SRB	Not Vulnerable	
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Vulnerable; contact TAC	
12.2SXE	Vulnerable; first fixed in 12.2(18)SXF9	12.2(18)SXF10
12.2SXF	12.2(18)SXF9	12.2(18)SXF10
12.2SXH	Not Vulnerable	
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Not Vulnerable	
12.2TPC	Not Vulnerable	
12.2UZ	Not Vulnerable	
12.2VZ	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	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	
12.2ZR	Not Vulnerable	
12.2ZU	Vulnerable; first fixed in 12.2(33)SXH available 31-Aug-07	12.2(33)SXH; available 31-Aug-07
12.2ZW	Not Vulnerable	
12.2ZY	Not Vulnerable	
Affected 12.3-Based Release	First Fixed Release	Recommended Release
There are no affected 12.3 based releases		
Affected 12.4-Based Release	First Fixed Release	Recommended Release
There are no affected 12.4 based releases		

Workarounds

If the IOS Secure Copy Server functionality is not needed then the vulnerability described in this document can be mitigated by disabling the Secure Copy server. The Secure Copy server can be disabled by executing the following command in global configuration mode:

```
no ip scp server enable
```

If the Secure Copy 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 "Improving Security on Cisco Routers" at <http://www.cisco.com/warp/public/707/21.html>. Please refer to the [Obtaining Fixed Software](#) section 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 a Secure Copy session with the device, which would allow the user to exploit this vulnerability.

Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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.

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 Vijay Sarvepalli from University of North Carolina at Greensboro.

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.

Distribution

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-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-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 1.0	2007-August-08	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)

Send

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](#).