

# Cisco Security Advisory: Cisco IOS Secure Shell Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20080521-ssh

<http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>

## Revision 1.1

Last Updated 2008 May 28 1600 UTC (GMT)

For Public Release 2008 May 21 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 Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. SSH is enabled any time RSA keys are generated such as when a http secure-server or trust points for digital certificates are configured. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier [CVE-2008-1159](#) has been assigned to this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>.

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

## ☐ Affected Products

### ☐ Vulnerable Products

Cisco devices running certain 12.4-based IOS releases and configured to be managed via SSH may be affected by this issue.

The IOS secure shell server is disabled by default. To determine if SSH is enabled, use the **show ip ssh** command.

```
Router#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

The previous output shows that SSH is enabled on this device and that the SSH protocol major version that is being supported is 2.0. If the text "SSH Disabled" is displayed, the device is not vulnerable. Possible values for the SSH protocol version reported by IOS are:

- 1.5: only SSH protocol version 1 is enabled
- 1.99: SSH protocol version 2 with SSH protocol version 1 compatibility enabled
- 2.0: only SSH protocol version 2 is enabled

For more information about SSH versions in IOS, please check the following URL: [http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t4/feature/guide/gt\\_ssh2.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ssh2.html).

The SSH server is not available in all IOS images. Devices that do not support SSH are not vulnerable. Please consult the table of fixed software in the Software Version and Fixes section for the specific 12.4-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 the 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 12.4(17):

```
Cisco IOS Software, C2600 Software (C2600-ADVENTERPRISEK9-M), Version 12.
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 07-Sep-07 16:05 by prod_rel_team

ROM: System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1

Router uptime is 1 week, 5 hours, 5 minutes
System returned to ROM by power-on
System image file is "flash:c2600-adventerprisek9-mz.124-17.bin"
```

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 SSH server feature enabled are not affected.

IOS-XR and IOS-XE images are not affected.

The following IOS release trains are not affected:

- 10-based releases
- 11-based releases
- 12.0-based releases
- 12.1-based releases
- 12.2-based releases
- 12.3-based releases

IOS releases prior to 12.4(7), 12.4(13d)JA, and 12.4(9)T are not affected by this vulnerability.

No other Cisco products are currently known to be affected by these vulnerabilities.

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

## ☐ Details

Secure shell (SSH) was developed as a secure replacement for the telnet, ftp, rlogin, rsh, and rcp protocols, which allow for the remote access of devices. The main difference between SSH and older protocols is that SSH provides strong authentication, guarantees confidentiality, and uses encrypted transactions.

The server side of the SSH implementation in Cisco IOS contains multiple vulnerabilities that allow an unauthenticated user to generate a spurious memory access or, in certain cases, reload the device. If the attacker is able to reload the device, these vulnerabilities could be repeatedly exploited to cause an extended Denial of Service (DoS) condition.

A device with the SSH server enabled is vulnerable.

These vulnerabilities are documented in Cisco Bug IDs:

- [CSCsk42419](#) ( [registered](#) customers only)
- [CSCsk60020](#) ( [registered](#) customers only)
- [CSCsh51293](#) ( [registered](#) customers only)

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

## ☐ 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 2.0.

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.

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>.

SSHv2 spurious memory access					
Calculate the environmental score of <a href="#">CSCsk42419</a>					
CVSS Base Score - <b>7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - <b>6.4</b>					
Exploitability				Remediation Level	Report Confidence
Functional				Official-Fix	Confirmed

SSHv2 spurious memory access
Calculate the environmental score of <a href="#">CSCsk60020</a>
CVSS Base Score - <b>7.8</b>

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
<b>CVSS Temporal Score - 6.4</b>					
Exploitability				Remediation Level	Report Confidence
Functional				Official-Fix	Confirmed

<b>Spurious memory access when SSH packets received</b>					
<b>Calculate the environmental score of <a href="#">CSCsh51293</a></b>					
<b>CVSS Base Score - 7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
<b>CVSS Temporal Score - 6.4</b>					
Exploitability				Remediation Level	Report Confidence
Functional				Official-Fix	Confirmed

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

## ☐ Impact

Successful exploitation of these vulnerabilities may result in a spurious memory access or, in certain cases, reload the device potentially resulting in a DoS condition.

[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) describes a release train and the platforms or products for which it is intended. 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/warp/public/620/1.html>.

IOS releases prior to 12.4(7), 12.4(13d)JA, and 12.4(9)T are not affected by this vulnerability.

<b>Major Release</b>	<b>Availability of Repaired Releases</b>	
<b>Affected 12.0-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.0 based releases		
<b>Affected 12.1-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.1 based releases		
<b>Affected 12.2-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.2 based releases		
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.3 based releases		
<b>Affected 12.4-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	12.4(13f) 12.4(16b) 12.4(17a) 12.4(18)	12.4(18b)
12.4JA	Only 12.4(13d)JA and 12.4(13d)JA1 are vulnerable, all other 12.4JA releases are not affected.	12.4(16b)JA3
12.4JK	Not Vulnerable	

12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JMC	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	12.4(16)MR2	12.4(16)MR
12.4SW	12.4(15)SW1	12.4(15)SW1
12.4T	12.4(9)T6 12.4(11)T4 12.4(15)T2 12.4(20)T	12.4(15)T5
12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	
12.4XC	Not Vulnerable	
12.4XD	Not Vulnerable	
12.4XE	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T5
12.4XF	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T5
12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T5
12.4XK	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T5
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Vulnerable; contact TAC	
12.4XW	12.4(11)XW6	12.4(11)XW6
12.4XY	Not Vulnerable	
12.4XZ	Not Vulnerable	

## ☐ Workarounds

If disabling the IOS SSH Server is not feasible, the following workarounds may be useful to some customers in their environments.

### Telnet

Telnet is not vulnerable to the issue described in this advisory and may be used as an insecure alternative to SSH. Telnet does not encrypt the authentication information or data; therefore, it should only be enabled for trusted local networks.

### VTY Access Class

It is possible to limit the exposure of the Cisco device by applying a VTY access class to allow only known, trusted hosts to connect to the device via SSH.

For more information on restricting traffic to VTYS, please consult:

[http://www.cisco.com/en/US/docs/ios/12\\_2/ipaddr/command/reference/1rfip1.html#wp1017389](http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/1rfip1.html#wp1017389).

The following example permits access to VTYS from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from anywhere else:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit host 172.16.1.2
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```

Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

### Infrastructure ACLs (iACL)

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The ACL example shown below should be included as part of the deployed infrastructure access-list, which will protect all devices with IP addresses in the infrastructure IP address range.

A sample access list for devices running Cisco IOS is below:

```
!--- Permit SSH services from trusted hosts destined
!--- to infrastructure addresses.
```

```
access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
```

```

!--- Deny SSH packets from all other sources destined to infrastructure addr

access-list 150 deny    tcp any INFRASTRUCTURE_ADDRESSES MASK eq 22

!--- Permit all other traffic to transit the device.

access-list 150 permit IP any any

interface serial 2/0
 ip access-group 150 in

```

The white paper titled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained here:  
[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_white\\_paper09186a00801a1a55.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml).

## Control Plane Policing (CoPP)

The Control Plane Policing (CoPP) feature may be used to mitigate these vulnerabilities. In the following example, only SSH traffic from trusted hosts and with 'receive' destination IP addresses is permitted to reach the route processor (RP).

**Note:** Dropping traffic from unknown or untrusted IP addresses may affect hosts with dynamically assigned IP addresses from connecting to the Cisco IOS device.

```

access-list 152 deny    tcp TRUSTED_ADDRESSES MASK any eq 22
access-list 152 permit tcp any any eq 22
!
class-map match-all COPP-KNOWN-UNDESIRABLE
 match access-group 152
!
!
policy-map COPP-INPUT-POLICY
 class COPP-KNOWN-UNDESIRABLE
  drop
!
control-plane
 service-policy input COPP-INPUT-POLICY

```

In the above CoPP example, the ACL entries that match the exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action are not affected by the policy-map drop function.

CoPP is available in Cisco IOS release trains 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T.

Additional information on the configuration and use of the CoPP feature can be found at the following URL:

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod\\_white\\_paper0900](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900):

## ☐ **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](mailto: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.

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

## ☐ **Exploitation and Public Announcements**

Cisco is releasing this IOS advisory out of our normal twice yearly cycle due to an increase in customer support cases linked to this bug. Cisco PSIRT has not received any reports of malicious exploitation.

This vulnerability was discovered by Cisco internal testing and customer service requests.

[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-20080521-ssh.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-teams@first.org](mailto:first-teams@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	2008-May-28	Content changes in these sections: Summary, Products Confirmed Not Vulnerable, and Exploitation and Public Announcements.
Revision 1.0	2008-May-21	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](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)