

Cisco Security Advisory: Cisco Service Control Engine Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20080521-sce

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

Revision 1.0

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

Three Secure Shell (SSH) vulnerabilities exist in the Cisco Service Control Engine (SCE) that may result in system instability or a reload of the SCE. The first vulnerability may be triggered during SSH login activity that is conducted within aggressive time frames. The second vulnerability may be triggered with normal SSH login activity in combination with other SCE management actions occurring simultaneously. The third vulnerability may be triggered during SSH login and is specific to the usage of unique invalid authentication credentials.

Cisco has made free upgrade software available to address these vulnerabilities for affected customers. There are no workarounds for these vulnerabilities.

Note: These vulnerabilities are independent of each other; a device may be affected by one vulnerability and not by the others.

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

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

☐ Affected Products

☐ Vulnerable Products

The SCE 1000 and 2000 series devices are affected by the following vulnerabilities if the SSH server on the SCE is enabled:

- System vulnerability to SSH login activity - affects SCE software versions prior to 3.1.6.
- SSH login activity leads to illegal Input/Output operations - affects SCE software versions prior to 3.0.7 and 3.1.0.
- SCE SSH authentication sequence anomaly - affects SCE software versions prior to 3.1.6.

Note: The SCE SSH server is disabled by default.

To determine whether you are running a vulnerable version of Cisco Service Control Operating System (SCOS) software, issue the "Show Version" command-line interface (CLI) command. The following example shows a Cisco SCE that runs software release 3.1.6:

```
SCE2000#>show version
```

System version: Version 3.1.6 Build 157
Build time: Mar 31 2008, 18:58:49 (Change-list 303626)
Software version is: Version 3.1.6 Build 157

☐ Products Confirmed Not Vulnerable

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

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

☐ Details

Cisco SCE 1000 and 2000 series devices provide high-capacity advanced application-level bandwidth optimization, stateful application inspection, session-based classification and control of network traffic. The SCE solution allows for the detection and control of network applications including: web browsing, multimedia streaming, and peer-to-peer (P2P).

This Security Advisory describes multiple distinct vulnerabilities. These vulnerabilities are independent of each other.

- System vulnerability to SSH login activity

A vulnerability impacting the SCE SSH server may be triggered during SSH login activity, resulting in system instability or a reload of the SCE. Specific SSH processes may encounter temporary resource unavailability if called within aggressive intervals.

This vulnerability is documented in Cisco Bug ID [CSCsi68582](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID [CVE-2008-0534](#).

- SSH login activity leads to illegal Input/Output operations

A second vulnerability exists in the SCE SSH server that may be triggered with normal SSH traffic to the SCE management interface occurring in conjunction with other management tasks. During this event, an illegal IO operation may impact the SCE management agent, requiring a reboot of the SCE to recover management access.

This vulnerability is documented in Cisco Bug ID [CSCsh49563](#) ([registered](#) customers only) and has been assigned CVE ID [CVE-2008-0536](#).

- SCE SSH authentication sequence anomaly

A third vulnerability exists in the SCE SSH server that may also be triggered during the SSH login process but unrelated to login attempt frequency or other concurrent management tasks. This issue is triggered by the usage of specific SSH credentials that attempt to change the authentication method, resulting in an authentication sequence anomaly impacting system stability.

This vulnerability is documented in Cisco Bug ID [CSCsm14239](#) ([registered](#) customers only) and has been assigned CVE ID [CVE-2008-0535](#).

[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>.

[CSCsi68582 - System vulnerability to SSH login activity](#) ([registered](#) customers only)

Calculate the environmental score of [CSCsi68582](#)

CVSS Base Score - **7.8**

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

<u>CSCsh49563 - SSH login activity leads to illegal I/O operations</u> (<u>registered customers only</u>)					
Calculate the environmental score of <u>CSCsh49563</u>					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<u>CSCsm14239 - SCE SSH authentication sequence anomaly</u> (<u>registered customers only</u>)					
Calculate the environmental score of <u>CSCsm14239</u>					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	

Functional	Official-Fix	Confirmed
------------	--------------	-----------

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

[-] Impact

Successful exploitation of these vulnerabilities may result in the loss of management access or, in some cases, cause vulnerable SCE devices to reload.

[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.

The following list contains the first fixed software release for each vulnerability:

Vulnerability	Affected Major Release	First Fixed Release
System vulnerability to SSH login activity	1.x	3.1.6
	2.x	3.1.6
	3.x	3.1.6
SSH login activity leads to illegal IO operations	1.x	3.0.7
	2.x	3.0.7
	3.x	3.0.7, 3.1.0
SCE SSH authentication sequence anomaly	1.x	3.1.6
	2.x	3.1.6

SCOS software version 3.1.6 contains the fixes for all vulnerabilities described in this document.

SCOS software is available for download from the following location on cisco.com:

- [SCOS 3.1.6](#) ([registered](#) customers only)

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

Workarounds

There are no workarounds for these vulnerabilities.

Filtering SSH traffic with Access Control Lists (ACLs) to affected SCE devices on the SCE management interface or on screening devices can provide a mitigation technique for these vulnerabilities. Restricting SCE SSH management interface access to only trusted devices through the use of SCE ACLs or Transit ACLs is strongly recommended.

Additional information about SCE ACLs is available in the "Configuring the Management Interface and Security" section of the SCE Software Configuration Guide: http://www.cisco.com/en/US/products/ps6134/products_configuration_guide_chapter09186a00808498b9.html#wp1060396

Additional information about tACLs is available in Transit Access Control Lists: Filtering at Your Edge: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

[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/warp/public/687/Directory/DirTAC.shtml> 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 vulnerabilities described in this advisory.

The SSH login activity vulnerability was discovered during the resolution of customer support cases.

The illegal Input/Output operation and authentication sequence anomaly were discovered by Cisco during internal testing.

[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-sce.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.

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

☐ Revision History

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. 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.](#)