



Cisco Content Security and Control Version 6.1.1587.0 Patch Release Notes

April 2007

Contents

This document provides release information for the Cisco Content Security and Control (CSC) Version 6.1.1587.0 patch release. It includes the following sections:

- [About the CSC 6.1.1587.0 Patch, page 1](#)
- [Installing the CSC SSM 6.1.1587.0 Patch, page 2](#)
- [Verifying the Installed Version of the CSC SSM Software, page 2](#)
- [Caveats, page 3](#)
- [Related Documentation, page 7](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 8](#)

About the CSC 6.1.1587.0 Patch

The CSC Version 6.1.1587.0 patch contains the following new feature:

- SMTP/TLS bypassing is configurable on the CSC SSM GUI. The default setting is disabled. To configure SMTP/TLS bypassing, choose **SMTP > Configuration > Advanced Settings**.

See the [“Resolved Caveats” section on page 6](#) for information about the caveats that have been resolved by this patch.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Installing the CSC SSM 6.1.1587.0 Patch

Install this patch only if you are running CSC SSM version 6.1.1569.0, version 6.1.1569.1, or version 6.1.1569.2. This upgrade applies only to the platform and versions previously listed. Existing user configuration and licenses will be preserved during the upgrade process. After the upgrade, the CSC version changes to 6.1.1587.0. All previous patch records are removed, because they are included in this upgrade.

To verify the version of the CSC SSM installed on the adaptive security appliance, see the [“Verifying the Installed Version of the CSC SSM Software” section on page 2](#).

To upgrade the CSC SSM, perform the following steps:

-
- Step 1** Download the `csc-p-6.1.1587.0.pkg` file from the Software Center on Cisco.com. You need to log into Cisco.com to download the software. If you do not have a Cisco.com account, visit the following website to become a registered user:
<http://tools.cisco.com/RPF/register/register.do>
 - Step 2** Access the Trend Micro CSC SSM console by performing the following steps:
 - a. Launch ASDM.
 - b. Choose **Configuration > Trend Micro Content Security**.
 - Step 3** Choose **Administrator > Product Upgrade** from the menu.
 - Step 4** Click **Browse** and select the `.pkg` file you downloaded.
 - Step 5** Click **Install**.
 - Step 6** Click **Summary** to confirm the installed software version.
 - Step 7** (Optional) Use an Eicar test file to confirm that the upgrade was successful and that the scanning services have been configured correctly.
-

For more information, see *Appendix A, “Reimaging and Configuring the CSC SSM Using the CLI,”* in the *Cisco Content Security and Control SSM Administrator Guide*.

Verifying the Installed Version of the CSC SSM Software

You can confirm the version of the CSC SSM software, and software components and patches from the ASA 5500 series adaptive security appliance CLI.



Note

The software version also appears on the summary page of the Trend Micro InterScan for Cisco CSC SSM interface.

To view the version of software installed on the CSC SSM using the CLI, perform the following steps:

-
- Step 1** To access the CSC SSM, open ASDM and click the **Content Security** tab.
 - Step 2** Choose **Tools > Command Line Interface** to display the Command Line Interface dialog box.
 - Step 3** In the command line field, enter the **show module 1 details** command, and then click **Send**.

The CSC SSM software version information appears.

```
hostname(config)# show module 1 details

Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:                ASA-SSM-20
Hardware version:     1.0
Serial Number:        0
Firmware version:     1.0(10)0
Software version:     CSC SSM 6.1.1587.0
MAC Address Range:    000b.fcf8.012c to 000b.fcf8.012c
App. name:            CSC SSM
App. Status:          Up
App. Status Desc:     CSC SSM scan services are available
App. version:         6.1.1587.0
Data plane Status:    Up
Status:               Up
HTTP Service:         Up
Mail Service:         Up
FTP Service:          Up
Activated:            Yes
Mgmt IP addr:         10.89.130.241
Mgmt web port:        8443
Peer IP addr:         <not enabled>
```

Caveats

This section describes the open and resolved caveats for the CSC SSM 6.1.1587.0 release. To view more information about an open or resolved caveat, use the Bug Toolkit on Cisco.com. If you are a registered Cisco.com user, access the Bug Toolkit on cisco.com at the following website:

http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml

To become a registered Cisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

For your convenience in locating caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are taken directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences, because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling and typographical errors may be corrected.

This section includes the following topics:

- [Open Caveats, page 4](#)
- [Resolved Caveats, page 6](#)

Open Caveats

Table 1 lists the caveats that are open in Version CSC 6.1.1587.0.

Table 1 **Open Caveats**

Cisco ID Number/ Trend Micro ID Number	Caveat Title
CSCsd05974/N/A	TCP flow dropped due to CSC card failure during SSM stress.
CSCsd17818/ CSC-SSM6.0-01004	Yahoo! Finance MarketTracker does not work.
CSCsd17889/ CSC-SSM6.0-00538	No notification displayed when downloading infected file from/to webmail.
CSCsd17954/ CSC-SSM6.0-01026	The HTTP proxy connection cannot tunnel through the CSC SSM.
CSCsd18011/ CSC-SSM6.0-01472	FTP file blocking will not work when file unscanned due to configuration.
CSCsd18030/ CSC-SSM6.0-01471	Connections may be interrupted during SSM service failure.
CSCsd18052/ CSC-SSM6.0-01470	E-mail notification from the CSC SSM is not received.
CSCsd18060/ CSC-SSM6.0-01473	With CSC enabled, large file transfers using HTTP/FTP or Windows Update fail.
CSCse12729/ CSC-SSM6.0-01474	The spyware pattern number may appear to be rolled back when you upgrade from 6.0 to 6.1.1519.0.
CSCse12745/ CSC-SSM6.0-01475	NRS feature may not be working within the first hour right after registration.
CSCse12755/ CSC-SSM6.0-01032	Some spyware may be detected even if Spyware category is not enabled.
CSCse12767/ CSC-SSM6.0-01201	Fails to convert non-UTF8 Japanese characters to UTF-8.
CSCse12772, CSCse12791/ CSC-SSM6.0-01196	Filename token may not be properly displayed in the e-mail inline insertion. Multi-byte filename may not be displayed correctly. These are duplicate defects.
CSCse12781/ CSC-SSM6.0-01193	Japanese strings may not be displayed correctly in system log messages.
CSCse12784/ CSC-SSM6.0-01209	Multi-byte strings are not allowed on the GUI.
CSCse12786/ CSC-SSM6.0-01476	Original e-mail may break if not encoded in UTF-8.
CSCsf05298/ CSC-SSM6.0-01272	Citrix not supported with CSC module.
CSCsf12514/N/A	CSC module needs to support TFTP blocksize option - RFC 2347 and RFC 2348.

Table 1 **Open Caveats (continued)**

Cisco ID Number/ Trend Micro ID Number	Caveat Title
CSCsf24483/ CSC-SSM6.0-01231	Activation code is invalid (CONTENT_ERR_AC_ILLEGAL) ERROR:1231.
CSCsf26197/ CSC-SSM6.0-01469	CSC software blocks Ameritrade streamer.
CSCsf98493/ CSC-SSM6.0-01264	VPN users using proxy have problem browsing via HTTP.
CSCsf98538/ CSC-SSM6.0-01253	White IP List on NRS will disappear from Trend UI.
CSCsg52819/ CSC-SSM6.0-01389	CSC module - Import function for user-defined domain lists.
CSCsg72210/ CSC-SSM6.0-01477	Trend URL filtering service does not currently support SOCKS-based proxy service.
CSCsg76794/ CSC-SSM6.0-01342	Last 30-day counter is not updating correctly.
CSCsg82181, CSCsh27090/ CSC-SSM6.0-01347	The flash image on www.cisco.com Home page sometimes cannot be loaded. (HTTP) Firefox 2.0 with faster plug-in has issue opening www.cisco.com. These are duplicate defects.
CSCsh15518/ CSC-SSM6.0-01374	Upgrading CSC module may result in inability to activate module.
CSCsh23475/ CSC-SSM6.0-01365	CSC module - URL blocking not functional for keywords.
CSCsh27011/ CSC-SSM6.0-01340	HP-UX FTP issues occur when in passive mode.
CSCsh27093/ CSC-SSM6.0-01350	(HTTP) URL filtering requests sent with incorrect format.
CSCsh27102/ CSC-SSM6.0-01353	Vulnerability for SSL.
CSCsh39788/ CSC-SSM6.0-01376	After upgrading CSC using a patch, URL filtering does not function.
CSCsh53472/ CSC-SSM6.0-01377	CSC module delays HTTP and FTP traffic.
CSCsh58901/ CSC-SSM6.0-01357	CSC Plus license expiration does not disable URL blocking in ASDM.
CSCsh58934/ CSC-SSM6.0-01363	SSM card becomes unresponsive after configuring via the ASDM.
CSCsh70101/ CSC-SSM6.0-01390	No error message for invalid URL blocking import file.
CSCsh80376/ CSC-SSM6.0-01359	Incorrect error message when URL rating lookup times out.
CSCsh97282/ CSC-SSM6.0-01406	CSC GUI admin port cannot be changed.

Table 1 Open Caveats (continued)

Cisco ID Number/ Trend Micro ID Number	Caveat Title
CSCsi05156/ CSC-SSM6.0-01404	CSC module increasingly delays TCP retransmissions.
CSCsi27604/ CSC-SSM6.0-01437	Sometimes when sending e-mails with attachments through the CSC, the body may be corrupted.
CSCsi40117/ CSC-SSM6.0-01436	100% CPU usage.
CSCsi43395/ CSC-SSM6.0-01397	Do not send disconnect-syslog when HTTP receives RST.

Resolved Caveats

Table 2 lists the caveats that have been resolved in Version CSC 6.1.1587.0.

Table 2 Closed Caveats

Cisco ID Number/ Trend Micro ID Number	Caveat Title
CSCsg32958/ CSC-SSM6.0-01316	SMTP/TLS can tunnel through CSC SSM starting with release 6.1.1569.0, but is not user-configurable.
CSCsg82152/ CSC-SSM6.0-01348	CSC jumps to 100% CPU usage, but new connections can be established and traffic scanned.
CSCsh27010/ CSC-SSM6.0-01337	POP3 never worked.
CSCsh31484/ CSC-SSM6.0-01379	Enabling email disclaimer insertion requires a valid Plus license.
CSCsh58836/ CSC-SSM6.0-01356	Unable to push pattern updates from Japanese TMCM console. Note This issue does not affect the English TMCM console.
CSCsh58911/N/A	CSC-SSM module CPU pegged at 100% usage.
CSCsh73881/ CSC-SSM6.0-01359	CSC SSM CPU usage at 100% when running 6.1.1569.1 image.
CSCsh74915/ CSC-SSM6.0-01391	CSC GUI does not redirect to Login page after a session timeout.
CSCsh90870/ CSC-SSM6.0-01369	Large POP3 e-mail downloads time out.
CSCsi06520/ CSC-SSM6.0-01405	FTP/TLS fails to negotiate through CSC and causes client to abort.
CSCsi07133/ CSC-SSM6.0-01396	TFTP client on CSC cannot transfer large files.

Table 2 **Closed Caveats (continued)**

Cisco ID Number/ Trend Micro ID Number	Caveat Title
CSCsi18226/ CSC-SSM6.0-01409	CSC GUI displays the following message even if failover is correctly configured: "InterScan for CSC SSM could not establish a connection because the failover peer is incorrectly configured to accept data from this host. Please verify failover settings on the peer, then try again."
CSCsi32093/ CSC-SSM6.0-01411	CSC SMTP/POP3 scanner may block e-mails with more than 100 recipients.
CSCsi40116/ CSC-SSM6.0-01435	CSC HTTP scanner may have issues with a few websites (e.g., OCLC) or cause 100% CPU busy.
CSCsi43391/ CSC-SSM6.0-01385	CSC control channel may time out under a heavy load and cause CSC to be taken offline or cause ASA failover.
CSCsi43393/ CSC-SSM6.0-01387	CSC may leak unused temporary file on flash disk in race condition.
CSCsi43397/ CSC-SSM6.0-01401	TMCM Agent log is not included in CSC Log export.
CSCsi43399/ CSC-SSM6.0-01438	CSC blocks AOL streaming.
CSCsi43791/ CSC-SSM6.0-01398	"dst cache overflow" kernel message is observed and CSC stops responding.
CSCsi52795/ CSC-SSM6.0-01358	Unable to unregister TMCM server if it is offline.
CSCsi52796/ CSC-SSM6.0-01366	Unable to enter a different Standard AC code on CSC GUI.
CSCsi52797/ CSC-SSM6.0-01394	The NRS Enable/Disable button on CSC GUI is not grayed out after Plus license expiration.

Related Documentation

For additional information, see the ASDM online Help or the following documentation found on Cisco.com:

- *Cisco Content Security and Control SSM Administrator Guide*
- *Cisco ASDM Release Notes*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

This document is to be used in conjunction with the documents listed in the “Obtaining Documentation, Obtaining Support, and Security Guidelines” section.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)

© 2007 Cisco Systems, Inc.
All rights reserved.