



Cisco Content Security and Control Version 6.1.1569.0 Patch Release Notes

November 2006

Contents

This document contains release information for the Cisco Content Security and Control (CSC) Version 6.1.1569.0 patch release. It includes the following sections:

- [About the CSC 6.1.1569.0 Patch, page 1](#)
- [Installing the CSC SSM 6.1.1569.0 Patch, page 2](#)
- [Verifying the Installed Version of the CSC SSM Software, page 2](#)
- [Caveats, page 3](#)
- [Related Documentation, page 6](#)
- [Obtaining Documentation and Submitting a Service Request, page 6](#)

About the CSC 6.1.1569.0 Patch

The CSC Version 6.1.1569.0 patch contains the following new features:

- Password reset, which allows you to reset the default CSC SSM password to “cisco.”
- A single password is required to access the CSC SSM GUI and CLI. For more information, see the *Cisco Content Security and Control SSM Administrator Guide*.
- Version numbering has been changed to reflect the software version number, build number, and patch release number. The format is as follows:
major software version.minor software version.build number.patch release number
- License renewal is available through the Cisco website.
- The TCP window size has been adjusted.
- The URL Reclassification Request has been changed to a web-based submission.



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

© 2006 Cisco Systems, Inc. All rights reserved.

- Workaround to CSCsd17818: Use the adaptive security appliance Modular Policy Framework to bypass CSC SSM scanning of website IP addresses.

See the “[Resolved Caveats](#)” section on page 5 for information about the caveats that have been resolved by this patch.

Installing the CSC SSM 6.1.1569.0 Patch

Install this patch only if you are running CSC SSM version 6.1-b1519 and version 6.1, patch 1. To verify the version of the CSC SSM installed on the device, 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-6.1.1569.0.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 doing the following:
- Launch ASDM.
 - 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 main 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** Use the `session` command to access the CSC SSM. Use `cisco` as the login name.
- ```
hostname(config)# session 1
```

```
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

```
login: cisco
Password:
```

```
Trend Micro InterScan for Cisco CSC SSM Setup Main Menu
```

```

1. Network Settings
2. Date/Time Settings
3. Product Information
4. Service Status
5. Change Password for Command Line Interface
6. Restore Factory Default Settings
7. Troubleshooting Tools
8. Reset Management Port Access Control List
9. Ping
10. Exit ...
```

**Step 2** Type **3** and press **Enter** to access the Product Information screen.

The Product Information screen displays the version and build number of each component of the CSC SSM. Installed patches appear below the component list.

```
Enter a number from [1-10]: 3
```

```
Product Information
```

```

Main version 6.1 build 1519
Mail component version 5.5 build 1118
Web component version 2.1 build 1154
Patches:
p-6.1-b1519-1 07/10/2006 22:31:14 CSC SSM 6.1 Patch 1
```

```
Press Enter to continue ...
```

**Step 3** Press **Enter**.

The Trend Micro InterScan for Cisco CSC SSM Setup Main Menu appears.

## Caveats

This section describes the open and resolved caveats for the CSC SSM 6.1.1569.0 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://tools.cisco.com/Support/BugToolKit/>

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 5](#)

## Open Caveats

Table 1 lists the caveats that are open in Version CSC 6.1.1569.0.

**Table 1**      **Open Caveats**

| ID Number  | Caveat Title                                                                                                               |
|------------|----------------------------------------------------------------------------------------------------------------------------|
| CSCsd05974 | TCP flow dropped due to CSC card failed during SSM stress.                                                                 |
| CSCsd17818 | Yahoo! Finance MarketTracker does not work. For a workaround, see <a href="#">About the CSC 6.1.1569.0 Patch, page 1</a> . |
| CSCsd17889 | Nothing seems to happen when downloading infected file from/to webmail.                                                    |
| CSCsd17954 | The HTTP proxy connection cannot tunnel through the CSC SSM.                                                               |
| CSCsd18011 | FTP file blocking will not work when file unscanned due to cfg.                                                            |
| CSCsd18030 | Connections may be interrupted during SSM service failure.                                                                 |
| CSCsd18044 | Connections may be interrupted during the SSM restarting period.                                                           |
| CSCsd18052 | E-mail notification from the CSC SSM is not received.                                                                      |
| CSCsd18060 | With CSC enabled, large file transfer using HTTP/FTP or Windows Update fail.                                               |
| CSCsd59143 | Modify e-mails sent by Trend CSC-SSM module to include device name, IP.                                                    |
| CSCse12729 | The spyware pattern number may appear to be rolled back.                                                                   |
| CSCse12745 | NRS feature is not working on the CSC SSM after registration.                                                              |
| CSCse12755 | Some spyware may be detected even if Spyware category is not enabled.                                                      |
| CSCse12767 | Fails to convert non-UTF8 Japanese characters to UTF-8.                                                                    |
| CSCse12772 | Filename may not be properly displayed in the e-mail inline insertion.                                                     |
| CSCse12781 | Japanese strings may not be displayed correctly in system log messages.                                                    |
| CSCse12784 | Multi-byte strings are not allowed on the GUI.                                                                             |
| CSCse12786 | Original e-mail may break if not encoded in UTF-8.                                                                         |
| CSCse12791 | Multi-byte filename may not be displayed correctly.                                                                        |
| CSCse89728 | Number of licensed seats shows a different value for Base and Plus licenses.                                               |
| CSCsf05298 | Citrix not supported with CSC module.                                                                                      |
| CSCsf12514 | CSC module needs to support TFTP blocksize option - RFC 2347, RFC 2348.                                                    |
| CSCsf26197 | CSC software blocks Ameritrade streamer.                                                                                   |
| CSCsf27606 | CSC software stops processing POP3 traffic.                                                                                |
| CSCsf28591 | CSC module generates compact Flash almost-full messages.                                                                   |

**Table 1** *Open Caveats (continued)*

| ID Number  | Caveat Title                                                                      |
|------------|-----------------------------------------------------------------------------------|
| CSCsf98493 | VPN users using proxy have problem browsing via HTTP: 1264.                       |
| CSCsf98538 | White IP List on NRS will disappear from Trend UI: 1253.                          |
| CSCsg25501 | Bypass filter for CSC module.                                                     |
| CSCsg28389 | HTTP scanner causes system to hit 100% busy.                                      |
| CSCsg52819 | CSC module - Import function for user-defined domain lists                        |
| CSCsg72210 | Trend URL filtering service does not currently support SOCKS-based proxy service. |
| CSCsg76794 | Last 30-day counter is not updating correctly.                                    |
| CSCsg82181 | Flash image on www.cisco.com home page sometimes cannot be loaded.                |

## Resolved Caveats

[Table 2](#) lists the caveats that have been resolved in Version CSC 6.1.1569.0.

**Table 2** *Closed Caveats*

| ID Number                | Caveat Title                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCse38627               | Last security event is overwritten by a POP3 or SMTP event.                                                                                                                       |
| CSCse67660               | Active Update failure messages may confuse customers.                                                                                                                             |
| CSCse71477               | CSC CPU and node counters are not displayed correctly in Japanese OS.                                                                                                             |
| CSCse78267               | Network Settings displayed on a running CLI Menu may not be updated right after importing configuration on CSC GUI, even if the new settings have been applied and are effective. |
| CSCse78267               | Gather Log feature on CLI Menu sometimes returns an error.                                                                                                                        |
| CSCse78267<br>CSCsf98485 | URL Filtering service does not support HTTP proxy.                                                                                                                                |
| CSCsf08627               | CSC/IPS Password Reset support has been added in ASDM 5.2.2.                                                                                                                      |
| CSCsf19517               | CSC Password screen Apply button is not enabled.                                                                                                                                  |
| CSCsf98459               | CSC CLI Menu and CSC GUI enforce different password lengths.                                                                                                                      |
| CSCsf98496               | URL Exception List does not allow more than 50 characters.                                                                                                                        |
| CSCsf98499               | "SMTP Incoming Domain" can be emptied.                                                                                                                                            |
| CSCsf98506               | Windows Update sometimes fails on corrupted ZIP detected.                                                                                                                         |
| CSCsf98519               | HTTP URL Filtering has a long timeout.                                                                                                                                            |
| CSCsf98551               | Change Trend service alias for receiving customer's submission of URL reclassification.                                                                                           |
| CSCsf98558               | "Check Status Online" on CSC GUI License window always updates "Last Status Check."                                                                                               |
| CSCsg19161               | CSC 6.1 is not detecting incorrect password entry.                                                                                                                                |
| CSCsg26887               | Incorrect TCMC config causes active update failure.                                                                                                                               |
| CSCsg28389               | CSC module 100-percent-CPU users cannot access network.                                                                                                                           |

**Table 2**      **Closed Caveats (continued)**

| ID Number  | Caveat Title                                                                                                 |
|------------|--------------------------------------------------------------------------------------------------------------|
| CSCsg31261 | Power cycle sometimes causes CSC to disable Mail filters.                                                    |
| CSCsg32958 | Unable to tunnel SMTP-TLS traffic through CSC.                                                               |
| CSCsg71856 | Unable to browse some websites, e.g., wisbar.org.                                                            |
| CSCsg72173 | Duplicate system log message is generated when multiple spyware applications are found in a compressed file. |
| CSCsg72185 | URL Filtering cache does not expire.                                                                         |
| CSCsg73233 | CSC GUI displays "Automatic synchronization is currently in progress" when failover configuration is saved.  |
| CSCsg73302 | Enter "<>" as URL Blocking rules on CSC GUI breaks GUI.                                                      |
| CSCsg73427 | The "View license detail online" link does not work.                                                         |
| CSCsg79130 | FTP EPSV EPRT options not working.                                                                           |
| CSCsg82129 | CSC jumps to 100% CPU and no new connections can be established.                                             |
| CSCsg82152 | FTP extension EPSV and EPRT did not work through CSC and are now blocked.                                    |

## 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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" 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, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Network 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. (0609R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

