



Cisco Content Security and Control Version 6.1(b1519-1) Patch Release Notes

July 2006

Contents

This document contains release information for the Cisco Content Security and Control (CSC) Version 6.1(b1519-1) patch release. It includes the following sections:

- [About the CSC 6.1\(b1519-1\) Patch, page 1](#)
- [Installing the CSC SSM 6.1\(b1519-1\) Patch, page 1](#)
- [Verifying the Installed Version of the CSC SSM Software, page 2](#)
- [Caveats, page 4](#)
- [Related Documentation, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 5](#)

About the CSC 6.1(b1519-1) Patch

The CSC Version 6.1(b1519-1) patch does not contain any new features. See the [“Closed Caveats” section on page 5](#) for information about the caveats that are resolved by this patch.

For information about the CSC 6.1(b1519) release, see the *Cisco Content Security and Control Version 6.1 Release Notes*.

Installing the CSC SSM 6.1(b1519-1) Patch

Install this patch only if you are running CSC SSM 6.1(b1519); your existing configuration and registration information will not be changed. If you are not sure what version of CSC SSM is installed on the device, see the [“Verifying the Installed Version of the CSC SSM Software” section on page 2](#).



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

© 2006 Cisco Systems, Inc. All rights reserved.

To upgrade your CSC SSM, follow these steps:

-
- Step 1** Download the csc-p-6.1-b1519-1.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:
- 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 are configured correctly.
-

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 command-line interface.



Note

The software version is also displayed 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 module using the command line interface, 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 6.1 release. To see more information about an open or resolved caveat, use the Bug Toolkit on Cisco.com. If you are a registered Cisco.com user, view 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>

This section contains the following topics:

- [Open Caveats, page 4](#)
- [Closed Caveats, page 5](#)

## Open Caveats

Table 1 lists the caveats that are open in Version 6.1(b1519-1)

**Table 1**      **Open Caveats**

| ID Number  | Caveat Title                                                              |
|------------|---------------------------------------------------------------------------|
| CSCsd05974 | TCP flow dropped due to CSC card failed during SSM stress.                |
| CSCsd17656 | The CSC SSM blocks the page with gzip displayed.                          |
| CSCsd17794 | If FTP-Inspection is disabled in the ASA CLI the FTP-data is not scanned. |
| CSCsd17818 | Yahoo! Finance MarketTracker does not work.                               |
| CSCsd17889 | Nothing seems to happen when downloading infected file from/to web mail.  |
| 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 | Email notification from the CSC SSM is not received.                      |
| CSCsd18060 | with csc enabled, Large file transfer on HTTP/FTP or Windows Update fail. |
| CSCse12745 | NRS feature is not be 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 email inline insertion.     |
| CSCse12781 | Japanese strings may not be displayed correctly in syslog messages.       |
| CSCse12784 | Multi-bytes strings are not allowed on the GUI.                           |
| CSCse12786 | Original email may break if not encoded in UTF-8.                         |
| CSCse12791 | Multi-bytes filename may not be displayed correctly.                      |
| CSCse68897 | Scheduled Update every 15 minutes doesn't sometimes start.                |

## Closed Caveats

Table 2 lists the caveats that were resolved in Version 6.1(b1519-1).

**Table 2**      **Closed Caveats**

| ID Number  | Caveat Title                                                         |
|------------|----------------------------------------------------------------------|
| CSCse61973 | CSC SSM does not store NULL HTTP header correctly.                   |
| CSCse74860 | Unable to import a configuration backup from one SSM to the other    |
| CSCse74868 | ESMTP AUTH response cannot pass through CSC                          |
| CSCse74885 | CSC runtime memory usage keeps increasing                            |
| CSCse74907 | High-frequency of SMTP disconnection syslogs is generated            |
| CSCse74913 | Some values reset to default on config import                        |
| CSCse74915 | Schedule update may not be executed every 15 minutes on some systems |
| CSCse74918 | Packet capture from CSC CLI Menu does not capture complete packet    |

## Related Documentation

For additional information, see the ASDM online Help or the following documentation located 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 Welcome to the Human Network 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, 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, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, 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. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.