Cisco IronPort Encryption Appliance 6.5.6 Release Notes

Published: June 3, 2013

Part Number: OL-29309-01

Contents

These release notes contain important information about running the latest version of the IronPort Encryption Appliance:

- **What's New.** This section describes new features introduced in this release. See What's New, page 2.
- **Fixed Issues**. This section describes the issues that were fixed in this release. See Fixed Issues, page 2.
- **Known Limitations**. This section describes known limitations in this release. See Known Limitations, page 5. Customers using AES encryption, please see defect CSCuh04303.
- **Patch Installation Instructions**. This section provides patch installation instructions for this release. See Patch Installation Instructions, page 6.
- **Service and Support**. This section provides information on obtaining service and support for your Cisco IronPort Encryption Appliance. See Service and Support, page 7.

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

What's New

This release focuses on fixing known issues and does not introduce new features.

Fixed Issues

The following table includes a description of the fixed issues in the latest version of the Cisco IronPort Encryption Appliance.

Table 1 Fixed Issue for the Cisco IronPort Encryption Appliance version 6.5.6.

Defect ID	Description
CSCug44025	**Fixed: Some envelopes opened in Chrome version 26 get a payload damaged error on decryption.** When attempting to decrypt some envelopes in version 26 of Chrome a "payload damaged" error is returned. This is caused by a payload decoding issue in the browser code. A workaround implemented in the envelope has resolved this issue. This problem does not occur on Chrome version 27 and higher.
CSCzv06965 76719	**Fixed: Non-ASCII filenames not displayed correctly in large file support (LFS).** When using large file support, attachment names containing non-ASCII characters are not displayed correctly. This issue has been resolved. **Note** Some older browsers do not fully support the use of non-ASCII characters. When the user is prompted to save an attachment to disk, some non-ASCII characters may not be displayed in the following browser versions: - Internet Explorer versions prior to IE9 - Firefox versions prior to Firefox 5 - Safari versions prior to Safari 6
CSCzv07836 71957	**Fixed: Admin GUI key Search Criteria Should Allow Exact Searches** In a previous release, the key search only allowed 'contains' searches which can take a long time and have performance implications. The ability to search exact strings has been added to improve this.
CSCzv08879 92056	**Fixed: Websafe attachments with names containing special characters cannot be accessed.** When websafe encounters a filename containing certain special characters (for example "/"), the file cannot be accessed. This could also have security implications when filenames contain paths. Special character escaping has been added to filename handling which resolves this issue.
CSCzv09009 76981	**Fixed: Attempting to resend undelivered secure messages fails** Fixed an issue in which attempting to resend undelivered secure messages failed. This occurred when the message delivery failed, and bounced messages were treated as errors rather than temporary failures.
CSCzv14847 74875	**Fixed: Cannot Open Certain Envelopes on IE7** Fixed an issue in which CRES users were unable to open envelopes, and "corrupted message" error displayed under the following circumstances: • If the envelope had one or more attachments • The envelope was large • Java was not installed on the user machine

Table 1 Fixed Issue for the Cisco IronPort Encryption Appliance version 6.5.6. (continued)

Defect ID	Description
CSCzv15585 83598	**Fixed: Apache Tomcat DoS vulnerability** Older versions of Apache Tomcat do not have a limit on the number of parameters that can be attached to a web request. An attacker can perform a POST to the WebServer which contains a very large number of requests which causes hash table collisions and therefore high CPU usage. The fix applied to the IEA Tomcat version adds an option to the admin GUI to limit the number of parameters on a request. The default value is 10,000.
CSCzv33183 63505	**Fixed: Password reset enhancements** Validation and escaping has been added to the add user form to ensure that scripting cannot be performed in these fields.
CSCzv36367 65895	**Fixed: TLS security advisory** An industry-wide vulnerability existed in the Transport Layer Security (TLS) protocol that could impact any Cisco product that used any version of TLS and SSL. The vulnerability existed in how the protocol handled session renegotiation and exposed users to a potential man-in-the-middle attack (This advisory is posted at *http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml*). This issue has been addressed for the Cisco IronPort Encryption Appliance.
CSCzv40527 75445	**Fixed: Login error erroneously informs customer the account is blocked** Fixed an issue in which a blocked account error message displayed for a suspended account. Because the steps to remedy a blocked account are different from the ones used to remedy a suspended account, the message may have caused difficulty in re-instating the account.
CSCzv42940 65937	**Fixed: Improved robustness for handling websafe properties files containing modifications** Fixed an issue in which when performing an upgrade, the upgrader was not designed to handle Websafe properties files which were modified.
CSCzv50875 80758	**Fixed: Secure Mailbox cleanup task can cause delays and block user access.** Currently the secure mailbox (websafe) cleanup task attempts to perform deletion of expired emails in a single SQL execution. This can cause delays in the delete task for large tables. During this time there is a lock placed on the content table and no users can access their mailbox. To resolve this issue, settings have been added to submit the cleanup task in configurable batches.
CSCzv53573 64785	**Fixed: Filename extension checking.** The IEA can be configured to reject attachments with a specified extension (such as .exe). In previous versions, the extension inspection was performed on the client side. Server side extension inspection has been added.
CSCzv54852 75478	**Fixed: Disable/Enable the Java-based File Transfer Applet (Uploader Applet) From the GUI** Once the Cisco IronPort Encryption appliance is upgraded to version 6.5.5, Java-based File Transfer Applet (Uploader Applet) will be disabled by default. To modify this setting, go to Admin UI > Configuration > Globals, “Enable File Transfer Applet.”
CSCzv57902 75872	**Fixed: Envelope Opener Applet does not load on first attempt on Internet Explorer 8** Fixed an issue in which when opening a secure envelope with an attachment for the first time, an error message displays and the message cannot be opened.
CSCzv59557 80858	**Fixed: Failure notifications are not processed properly when next app is not null.** When the next application for a rule is set (not null), and a failure occurs (for example, quota exceeded) the failure notification is not processed properly. The failure notification should be sent to the configured recipients, but instead it is processed by the next application specified. This issue has been resolved.

Table 1 Fixed Issue for the Cisco IronPort Encryption Appliance version 6.5.6. (continued)

Defect ID	Description
CSCzv60679 75892	**Fixed: Database table size issues may occur when tracking is enabled** Fixed an issue in which the T_TRACKINGRECIPS table was not cleaned up by the Tracking Cleanup scheduled task, possibly leading to excessive database size. Now the table is cleaned up by the Tracking Cleanup scheduled task.
CSCzv61271 71729	**Fixed: Socket exception information** In the previous releases, the following socket exception was reported at ERROR level: ***ERROR [org.apache.tomcat.util.net.PoolTcpEndpoint] Remote Host /<IP Address>*** ***SocketException: Connection reset*** Now, if there is a socket exception when a server is restarted, the exception is displayed as INFO along with the stack trace.
CSCzv63338 77686	**Fixed: Updated version of OpenSSH** Updated the OpenSSH version to openssh-4.3p2-72.el5_6.3 to fix the security vulnerability listed in CVE-2008-5161.
CSCzv63614 81897	**Fixed: "Unknown Command" Error Occurs When Secure Reply Times Out** When using the secure reply function, if the page times out an "unknown command" error is presented to the user. This issue has been resolved. Now when the page times out the user is prompted to enter username and password.
CSCzv65491 65623	**Fixed: Email messages sent using the Send Secure button with multiple compose windows were not encrypted.** Fixed an issue in which if multiple email messages were being composed simultaneously and the **Send Secure** button was used to send more than one of the email messages, an error condition sometimes occurred where only the first email message sent was successfully encrypted.
CSCzv68909 77577	Support was added to allow mobile device users to cache credentials in the form of a cookie so that users do not need to enter their credentials each time they open secure envelopes from their mobile devices. **Note** By design, high security envelopes do not cache credentials. To use this feature the envelope security must be set to medium or lower.
CSCzv70904 65740	**Fixed: Java SE Critical Update for vulnerabilities.** The latest JRE update is 45 and is included in this version. For details see: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
CSCzv76128 64930	**Fixed: Sometimes secure mailbox messages are not stored encrypted although encryption is enabled.** Although encryption was enabled in the web services properties, not all messages were stored encrypted. Previously, encryption could be enabled via the SMTP Adapter ruleset. This is now disabled and only the settings in Webservices > Websafe > Content Encryption will take effect. **Note** This will also effect any archiving rules.

Table 1 Fixed Issue for the Cisco IronPort Encryption Appliance version 6.5.6. (continued)

Defect ID	Description
CSCzv87365 86776	**Fixed: Request forgeries vulnerability** A scenario was found in which an authenticated admin could inadvertently execute a forged request. This issue has been resolved.
CSCzv93806 64086	**Fixed: Optimize the Envelope Open Process** Optimize the envelope opening process so that the user is prompted for credentials earlier and decryption is faster.

Known Limitations

The following table includes descriptions of known issues in the latest version of the Cisco IronPort Encryption Appliance.

Table 2 Known Issues for the Cisco IronPort Encryption Appliance version 6.5.6.

Defect ID	Description
CSCzv00213 73128	**When attempting to attach files using the Java-based File Transfer Applet (Uploader Applet), clicking the *Done* button while file uploads are in progress aborts any uploads in progress** When attempting to attach files to an encrypted message, clicking the Done button causes the process to abort, and changes are lost.
CSCzv23201 72918	**SMTP adapter is dependent upon scheduler service** The Scheduler Service must start before the SMTP adaptor can start. The SMTP adapter is responsible for processing mail, so email may not be sent or received after server startup. This dependency can be removed through manual configuration. Please contact customer support if you encounter this problem.
CSCzv30367 76309	**Individual file size limits are not checked when uploading files** When uploading files during message composition, the individual file size is not checked. However, total message size limits are still working as expected. For example if the file size limit is 25 MB per file, and 50 MB for the total message size, the Cisco IronPort Encryption appliance would allow you to upload a 30 MB file, but it would not allow the total message size to exceed 50 MB.
CSCuh04303	**AES envelopes cannot be decrypted** Envelopes created with AES encryption cannot be decrypted. After credentials are entered, and a message is displayed saying “Contacting server. Please wait...,”nothing occurs with the envelop. However, a JavaScript error is written to the browser log file.
CSCzv32234 79216	**The “Forget Me on this Computer” field not present when the “Remember Me” checkbox is checked and message is opened via the Open Online link** When decrypting a message using the Open Online link while the “Remember Me” checkbox is checked, the “Forget Me on this Computer” link is not present. **Workaround**: Uncheck the “Remember Me on this computer” checkbox or delete all cookies pertaining to the IEA hostname.

Table 2 Known Issues for the Cisco IronPort Encryption Appliance version 6.5.6. (continued)

Defect ID	Description
CSCzv40802 72907	**Temporary files are not removed if the application server is restarted before the user session times out** When opening an envelope, temporary files that are created do not get removed if the application server is restarted before the user session times out. This can cause memory problems if the temporary directory becomes large.
CSCzv44158 76705	**Java-based File Transfer Applet (Uploader Applet) does not warn when attachment process is aborted** When adding attachments using the Java-based File Transfer Applet (Uploader Applet), if the Done button is clicked before the files finish uploading, the files do not get attached and no warning displays to notify customers that the files are not attached.
CSCzv50579 62168	**Unable to modify some users whose account name contains special characters** After entering a new user whose account name contains special characters, an error may appear stating that the user information cannot be modified.
CSCzv57708 73127	**When attempting to attach multiple files using the Java-based File Transfer Applet (Uploader Applet), clicking the *Remove* button causes the page to reset and attachments are lost** When attempting to attach multiple files to an encrypted message, if you click the *Remove* button, this causes the page to reset and all attachments to be lost.

Patch Installation Instructions

Follow the instructions below to obtain and install the patch.

Pre-installation Requirements

Before you upgrade to the 6.5.6 version of the Cisco IronPort Encryption Appliance, verify that the appliance meets the following requirements:

- **Check for class-mapping.properties file customizations**. The class-mapping.properties file is modified as part of this upgrade. Any customizations to this file will be overwritten, and will need to be reinstated after the upgrade. The default class-mappings.properties is located in /usr/local/postx/server/conf/websafe. Any class-mappings.properties files which exist outside of this directory contain customizations. These customizations will need to be identified as part of the upgrade and added again after the upgrade is complete.
- **Shell Access on Cisco IronPort Encryption Appliance**. You must have access to the shell for the Cisco IronPort Encryption Appliance. For more information, refer to Chapter 1, “Setting Up the Cisco IronPort Encryption Appliance,” in the *Cisco IronPort Encryption Appliance 6.5 Installation Guide*.

- **Version**. You must have one of the following versions of the Cisco IronPort Encryption Appliance:
  - 6.5.4.1.2
  - 6.5.4.2
  - 6.5.5
  - 6.5.5.1
  - 6.5.5.2
  - 6.5.5.2.1
  - 6.5.5.3
  - 6.5.5.4
  - 6.5.5.5

  To verify the version, log into the appliance at the CentOS command prompt, and select option a - About from the main menu.
- **Internet access from Cisco IronPort Encryption Appliance**. You must be able to access the Internet from the Cisco IronPort Encryption Appliance. Internet access is required to download the tools that are necessary to install the patch.

Installation Steps

Step 1 Use the following command to copy the software patch from the IronPort Support Portal to your appliance:

```
scp checksum_iea_6.5.4.2_6.5.4.1.2_6.5.5x-6.5.6_patch.sh admin@<IEA IP Address>:
```

Step 2 Use SSH to connect to the appliance.

```
ssh admin@<IEA IP Address>
```

Step 3 At the main menu, enter option x to exit to the Unix command prompt.

Note The x option is a hidden command and does not appear in the list of menu options

Step 4 Use the following command to install the patch:

```
sh ./checksum_iea_6.5.4.2_6.5.4.1.2_6.5.5x-6.5.6_patch.sh
```

Step 5 Type exit to return to the main menu for the Cisco IronPort Encryption Appliance.

Step 6 To verify that the patch was properly installed, select option a - About from the main menu. If the patch installation was successful, the software version number is displayed as version 6.5.6.

Service and Support

You can contact Cisco Customer Support using one of the following methods:

- Cisco Support Portal: http://www.cisco.com/support
- Phone support: Contact Cisco Technical Assistance Center (TAC) within U.S. /Canada at 800-553-2447 and at Worldwide Phone Numbers.

- Email: tac@cisco.com

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.