Release Notes for Sourcefire SSL Appliances SSL1500, SSL2000, and SSL8200 v3.7.3

First Published: August 25, 2014
Sourcefire SSL Appliance v.3.7.3

Update Notification

This is a maintenance release for the SSL1500, SSL2000, and SSL8200 systems. See Resolved Issues, page 2 for information on all resolved issues.

The files associated with this patch release are:

- `sslv-3.7.3-8-sourcefire.patch`
- `sslv-3.7.3-8-sourcefire.nru`

The upgrade mechanisms described below can be applied to any system that is running Version 3.7.1-71 software.

The patch mechanism will not update the rescue image in the system. Hence, if you ever use the **restore factory defaults** option, the appliance will be re-imaged with the version of the rescue image. At that point you will need to re-apply the patch.

Following the patch upgrade, customers are advised to upgrade the rescue image to v3.7.3 by applying the `sslv-3.7.3-8-sourcefire.nru`.

Applying the Patch

To apply the patch, access the ***platform*** **> Update** menu option on the web interface, then select the `sslv-3.7.3-8-sourcefire.patch` file, and click **OK**.

Your existing configuration data and existing logs, etc., will be preserved during the patch upgrade.

Cisco Systems, Inc.
www.cisco.com

Applying the NRU

To apply the `.nru` file to update the rescue image, access the ***platform*** **> Update** menu option on the web interface, then select the `sslv-3.7.3-8-sourcefire.nru` file, and click **OK**.

The existing rescue image will be replaced with the new 3.7.3 image.

Resolved Issues

- Resolved an issue in which the SSL Visibility appliance became unusable and GUI timeouts occurred when navigating screens, requiring a manual reboot of the appliance to recover.
- Resolved a memory leak in the SSL intercept engine, when processing SSL flows with a large numbers of unique X.509 certificates. The issue resulted in no SSL sessions being inspected, and sometimes caused a restart.
- Resolved an issue where IP fragments would not pass successfully through the SSL Visibility Appliance.
- Resolved an issue where incorrect processing of IP fragments sometimes lead to a crash requiring a manual restart.
- Resolved an issue that resulted in NFE 0 overload messages and caused the SSL Visibility Appliance to stop decrypting.
- The SSL Debug log now rotates correctly. Previously, debug logs could fill up the internal disk.
- Addressed OpenSSL vulnerability CVE-2014-0224.
- Resolved an issue that prevented proper startup of the appliance after a patch upgrade.

Known Issues

- The SSL Appliance is unable to inspect traffic to some Google sites from Chrome on Windows, due to a proprietary TLS extension. Sessions that meet these characteristics are cut through by the SSL Appliance. The Session Log Status will show: `Unsupported TLS extension`.
- First-time boot may take up to five additional minutes if no network cable is plugged into the management network port.
- Patch upgrades do not update the default external CA list. New external CAs can be installed using the provided PKCS#7 file. Refer to the Important Information section for more details.
- The vSphere VNC client sends an unencrypted ClientHello message, resulting in `Corrupt Record` session errors.
- The web interface panel that notifies users to reboot the appliance after a configuration change disappears after the user has logged out.
- Diagnostic files generated via the command line are deleted when the user logs out or the SSH session is terminated. The diagnostics files should be downloaded as soon as possible and before logout.
- The following characters are not allowed in alert e-mail addresses: !, #, $, %, &, ‘, *, +, /, =, ?, ^, `, {, }, |, ~

- A half-duplex connection is negotiated if the SSL Appliance is connected to a 1000 Mbps port that is forced to operate at 100 Mbps. Note that a full-duplex connection is negotiated if connected to a 100 Mbps port or a 1000 Mbps port running at full speed.
- DER-formatted keys and certificates cannot be used as web UI certificate/keys.
- The SSL Appliance may sporadically not send `ClientHello` messages of cut-through flows to the attached appliance.
- The **Replace Certificate and Key** rule action is not supported for SSL flows using ECDSA authentication.
- TCP connections with a small receive window may fail when a large amount of data is added to the flow.
- SSL sessions to the ThreatPulse service may occasionally be rejected due to cryptographic operation errors.
- Maximum throughput performance of UDP traffic is affected when a small number of UDP flows is used.
- SSL Inspection is not supported for SSL flows using some experimental TLS protocol extensions. Refer to Important Information section for more details.
- The SSL Appliance SSL8200 model will try to boot from a USB stick if you insert into the front USB port.
- Deactivating an Active Inline segment may cause some packets to be received and re-transmitted on the device ports in an endless loop. Workaround: Pull out and re-insert the cable on the deactivated segment.
- DER-encoded PKCS#8 keys cannot be imported into the PKI store.
- The SSL Appliance cannot process SSL renegotiation on inspected SSL flows and will terminate such flows. Cut-through policy rules must be used to prevent flow termination.
- Policy activation failure on single segment causes policy activation failure on all other segments. Furthermore, policy errors in rulesets not used by active segments will also prevent policy activation.
- The default list of external certificate authorities includes CA certificates signed using the deprecated MD5 hash algorithm.
- Timestamps in remote system log entries have one-second resolution and do not include fractions of seconds.
- SSL error counts and invalid certificate information is cleared when the appliance policy is reactivated.
- All platform configuration changes require rebooting the SSL Appliance to take effect.
- The SSL session log may show sessions with harmless `Alert[C]: unknown (0)` error messages.
- The SSL appliance does not correctly match policy rules to SSL flows that contain non-ASCII characters in the **Subject** and **Issuer** server certificate fields.
- Disabling a Remote Logging entry causes the options configured in the entry to be lost.
- The command line diagnostic interface cannot be used during the bootstrap phase to set IP configuration on the management network interface. Use the front panel LCD instead.
- System log files are rotated once per-day regardless of the size of the file and only removed after a month.
- SNMP traps for link loss may not be generated if the link is recovered within 30 seconds.

- Manually failed segments are automatically unfailed when the SSL Appliance is rebooted.
- OCSP is not supported for server certificate validation. Only manually loaded CRLs can be used.
- Installing a valid SSL Visibility license may cause a brief loss of connectivity while unfailing the port configured on active segments. This is an issue on only the SSL1500.
- If two or more instances of the web interface are opened in different tabs or windows of the same browser on the same computer, logging out of one instance causes the user to be logged out of all other instances.
- When manually changing the date and time, the new time is set only when the platform configuration changes are applied.
- Some SSL sessions might fail with invalid SSL MAC calculations. This usually indicates that packets on the wire are corrupt, or have been tampered with.
- Restoring a policy that contains active segments does not always activate the segments. Workaround: Manually activate the segments.
- PKI objects (certificates or keys) can be removed even if they are referenced by the active policy.
- If more than one administrator are making changes to the SSL appliance configuration, they will have to log out and log in again before changes made by the other person will be reflected in the user interface.
- A segment configured to use any the Active-Inline (AI) modes will, under load, reject some SSL sessions because of packet feedback timeouts. This means that decrypted packets sent to the attached FireSIGHT System device did not return in time to complete the feedback loop required to trigger a re-encrypt of the original packets.
- A TCP FIN/FIN-ACK/ACK sequence is generated at the end of each decrypted SSL session. The three packets in this sequence might arrive at the attached FireSIGHT System device out of sequence. This should not pose any problems for TCP reassembly devices.
- The system log is currently displayed in oldest-to-latest order, and updates will only be reflected on the last page, and only after pressing the Last button.
- Internal CA certificates are not automatically checked for expiration. Workaround: Periodically check the certificates on the user interface.
- Only network interfaces used by active segments will change color on the user interface dashboard, based on the status of the interface. This is an issue for only the SSL1500.
- The SSL session log currently captures all flows that look like SSL, even though the flow might not be SSL – this is known as a false-positive. Each session log entry also contains a flag that indicates whether the session has been confirmed as valid SSL, specifically whether the policy decision has been applied to the session. This flag is not displayed on the user interface, but SSL session log post-processing tools can use this flag to filter out all the false-positives.
- When an SSL Appliance recovers from an overload condition it may flag some SSL sessions with the `Invalid cryptographic response` error code.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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