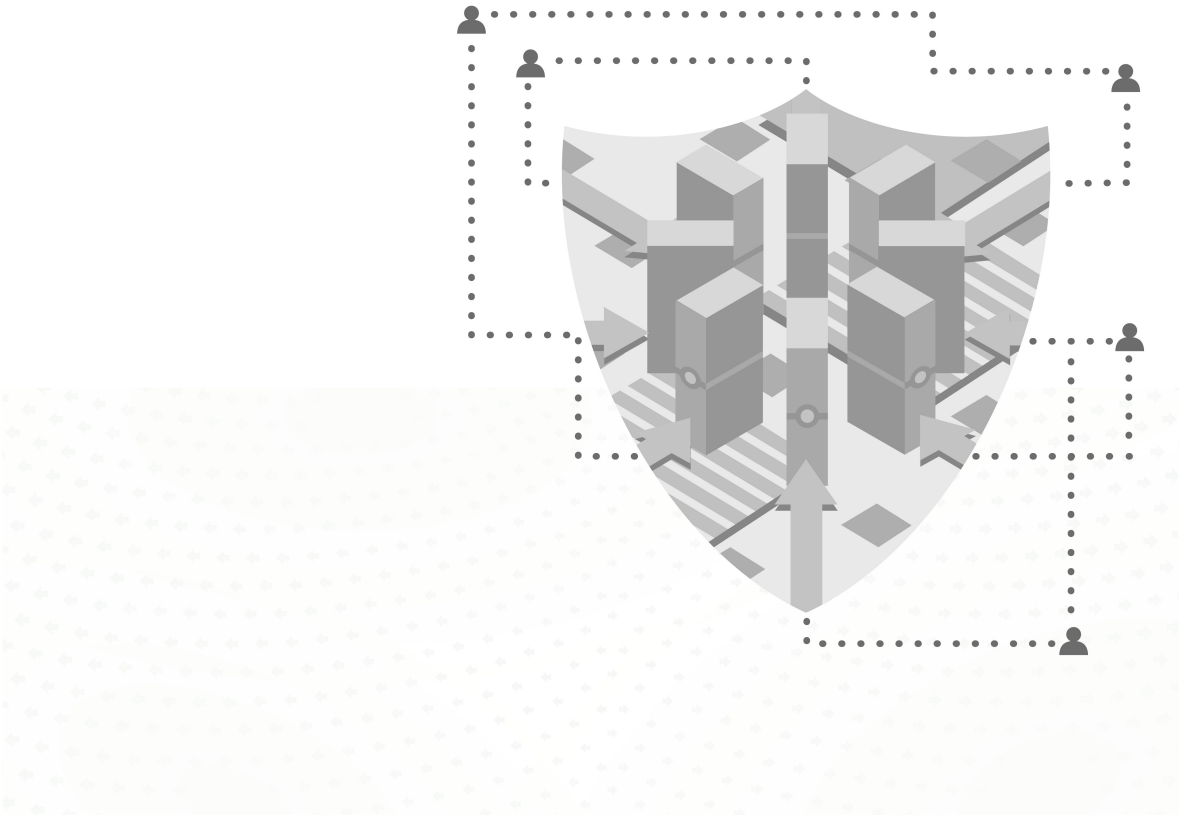
Sourcefire
SSL Appliance 1500, 2000, 8200
Release Notes

Software v. 3.7.1-71
Document Revision: 05/20/2014



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

1. Upgrading Sourcefire SSL Appliances from Version 3.6 to Version 3.7.1-71

This document provides instructions for upgrading installations of the Sourcefire SSL appliance from version 3.6.x to version 3.7.1-71. This is performed in two steps:

1. Upgrade from version 3.6.x to version 3.7.1-70, as described in Section 2.
2. Upgrade from version 3.7.1-70 to version 3.7.1-71, as described in Section 3.

Version 3.7.1-71 is a security patch release which addresses the HeartBleed exploit, protecting against it for SSL traffic passing through and inspected by the Sourcefire SSL appliance. This patch allows you to protect internal servers and prevent vulnerable client systems from attack even if they visit a malicious SSL server.

NOTE: To protect your Sourcefire SSL appliance from the HeartBleed exploit, you must apply both system upgrades listed above, in the order shown.

2. Upgrading Sourcefire SSL Appliances from Version 3.6 to Version 3.7.1-70

2.1 Update Description

This major release for the SV1800, SSL2000 and SSL8200 systems provides a number of new features and capabilities as well as fixing a number of important bugs. Customers are strongly recommended to upgrade to this release if they are running any earlier versions of the software.

The patch upgrade mechanisms described below can be applied to any system that is running version 3.6.x software. If you have a system running an earlier version, you **must** upgrade to a v3.6.x release before installing the 3.7 patch.

The files associated with this release are:

- sslv-3.6-to-3.7.1-70-sourcefire.patch
- sslv_3.6.3_to_3.7.0_ca_certificates.p7b

2.1.1 Upgrading the Sourcefire SSL Appliance

Upgrading the Sourcefire SSL appliance to software version 3.7 is straightforward. Before you begin:

- Make sure the appliance is running software version 3.6.x; upgrade the unit to 3.6.x if it is running older software.
- As a precaution, back up all configuration and policy data before the upgrade.

When you are ready to proceed:

1. Access the **(platform) > Update** menu.
2. Use the Choose File button to select the upgrade file, then press OK.
3. Reboot the appliance when prompted.
4. Wait for the upgrade to complete. This may take several minutes, and involves the appliance rebooting a number of times.

5. When the Sourcefire SSL appliance has reconnected, if you have subscribed to the Host Categorization feature, install the Host Category license. For more information, see the administration and deployment guide for your device.
6. Import the PKCS#7 encoded external CA certificate file (see Section 2.2, *Important Information*).

The following items will automatically be restored after the upgrade:

- System log
- Management configuration (NTP, hostname, IP, timezone, date, remote syslog)
- Policy (rulesets and segment definitions)
- PKI store
- User database
- Alerts configuration
- Remote authentication configuration

The following items will **not** be preserved:

- SSL session log
- SSL statistics
- Platform statistics (CPU, memory, disk utilization, temperatures, fan speeds)
- External interface statistics

2.1.2 Downgrading the Sourcefire SSL Appliance

In the unlikely event you want to downgrade from 3.7, contact Customer Support for assistance.

2.2 Important Information

- After a 3.6.x to 3.7.1 upgrade, or after restoring a 3.6.3 PKI store backup, the list of external CA certificates will not include the CA certificates added in the 3.7.1 release. Without the new list of external CA certificates, the X.509 status for some sites (for example, www.google.com) will be "Invalid Issuer." The following PKCS#7 encoded file should be imported to update the external CA list: sslv_3.6.3_to_3.7.0_ca_certificates.p7b.

  Be sure to backup the PKI store after importing the CA certificates. Note that the system log will have many warnings about duplicate entries; these log entries can be safely ignored.
- Google has recently introduced an undocumented proprietary TLS extension that is used when the Chrome browser connects to Google sites over TLS. The Sourcefire SSL appliance is unable to inspect TLS sessions using the proprietary extension, but will detect the presence of the TLS extension and apply the action specified by the per-segment Undecryptable Actions, specifically the action for "Cipher Suite".
- Most applications making TLS connections have an embedded list of trusted CA certificates, and some of those applications do not expose a mechanism to modify the trusted CA certificate store, which makes it impossible to inspect TLS sessions originating from those clients. Examples of such clients applications are: Skype, Evernote, Dropbox. Attempting to decrypt those sessions will likely result in a fatal SSL alert in the SSL session log, such as "Alert[C]: certificate unknown" or "Alert[C]: bad certificate."

- The **(Monitor) > Errors** screen shows counts of error codes since the last policy activation, which means that the error code list is cleared as soon as any changes to the policy and/or PKI store is committed. The implication is that the value in the **#Error** column on the **(Monitor) > SSL Statistics** page does not correspond with the sum of the error counts shown on the **(Monitor) > Errors** screen.
- The **Host Categorization** feature utilizes a local database of categories downloaded from Blue Coat servers. There might be a discrepancy in the category according to the local database when compared to the result on http://sitereview.bluecoat.com. Over time the local database will be updated with the latest confirmed categories on Blue Coat servers.

2.3 Enhancements and New Features

- Host categorization support enables category-based policies; you can write rules which are triggered by category matches. This optional feature requires a subscription license; if an installed license expires, policy will run, but you will see a category value of '*Unlicensed*.' For information on installing a Host Category license, see the administration and deployment guide for your device. The first matched category will be logged in the SSL session log details.
- Server Name Identification (SNI) and Subject Alternative Name (SAN) support is added to policies, reflected in the renaming of the **Distinguished Name** and **Common Name Lists** to **Subject/Domain Name** and **Domain Name Lists**. Existing policies will be automatically updated to use the new naming conventions. Both the SAN and SNI information are captured in the SSL session log details, and the SNI will be displayed with the prefix "SNI:" in case the domain name is not available (missing from X.509 information); typically, this will be for a re-used SSL session.
- X.509 Subject Alternative Name (SAN) information is now displayed for all items in the PKI store.
- The EULA and software attributions information can now be accessed from the UI login screen.
- The list of external X.509 CA certificates bundled with the appliance now includes the latest root CA certificates from major browsers. Refer to See Section 2.2, *Important Information,* for more details.
- Basic jumbo frames support; jumbo frames now cut through, so you no longer need to redirect jumbo frame traffic to avoid corruption.
- A command line diagnostic interface, accessed via serial or SSH session, helps you troubleshoot issues. Customer Service may request you compile a diagnostics report or perform other actions. The diagnostics interface is very useful if you cannot access the WebUI.
- The SSL session log now displays fatal SSL alerts received from endpoints. The alerts are indications that the endpoint SSL stack had a failure, and is not necessarily indicative of a failure in the Sourcefire SSL appliance. Refer to See Section 2.2, *Important Information,* for more details.
- The SSL session log now only logs entries after the SSL handshake has completed, compared to previous versions that logged the entries as soon as the policy decision was made. The advantage is that errors in the SSL handshake are logged as one SSL session log entry, instead of as an update on an existing SSL session log entry.

- The ruleset activation logic was changed to prevent segment activation if any inconsistencies were found from parsing the ruleset. The advantage is that invalid rules are caught at activation time.
- Support added for AES-GCM and ChaCha20-Poly1305 cipher-suites, as well as TLS heartbeats.
- The "Decrypt (Key known)" action has been removed because of the confusion caused when comparing it to the "Decrypt (Certificate and Key known)" action.
- Session log data now optionally sent to remote syslog server. You may select to send one of these sets of messages to each enabled syslog server:
    - Appliance Logs
    - Appliance Warning/Error Logs
    - Session and Appliance Logs
    - Session and Appliance Warning/Error logs

  Make sure to select the correct **Session Log Mode** on the activated Segments as well.
- The number of remote syslog servers supported increased to eight in the **(platform) > Remote Logging** menu.
- **System Log** entries are now rate-limited to a maximum of 60,000 messages in a 3 second period.
- SSL **Session Log** entries now log the matched rule index, and can be viewed in the SSL session log details. This enhances the mechanism to debug rulesets.
- The cut-through performance of small Ethernet frames has been improved.
- Incomplete or broken SSH sessions will time out after 45 seconds (STIG NET1645).
- The major subsystems in the appliance were upgraded to the latest firmware versions, and the base operating system was updated to a long-term-support version of Linux. The UI web server was also updated to prevent recent vulnerabilities.
- Customers have the option of specifying the management network IP address on the front panel (keypad and LCD). The default address is now 0.0.0.0.
- In versions prior to 3.7 a restriction was enforced to only accept a custom X.509 UI certificate if the common name (CN) in the certificate matched the hostname of the Sourcefire SSL appliance. This restriction has been removed, allowing the customer to install a customer UI certificate before setting the hostname of the appliance.
- The TACACS+ privilege level to Sourcefire SSL appliance security role mapping was changed to the following:

  0 = Auditor

  1 = Auditor + Manage Appliance

  2 = Auditor + Manage Policy

  3 = Auditor + Manage Appliance + Manage Policy

  4 = Auditor + Manage PKI

  5 = Auditor + Manage Appliance + Manage PKI

  6 = Auditor + Manage Policy + Manage PKI

  7 = Auditor + Manage Appliance + Manage Policy + Manage PKI

- More advanced POST integrity checks were added to increase the security of the appliance.
- Improved the mechanism used to determine the appliance hostname after a DHCP lease is acquired.
- Improved TCP retransmit handling for certain TLS1.1/TLS1.2 cipher-suites using RSA key exchange
- Various functions of the appliance can now utilize the SCP protocol (Linux:scp or Windows:pscp.exe). For example, packet captures and diagnostics archives can be downloaded directly from the appliance using SCP. The appliance can also be updated remotely by uploading a patch file to **[user]@[appliance]:update** (the appliance must still be rebooted from the UI or diagnostics interface for the update to be applied).

2.4 Issues Resolved

- Fixed a crash in generating the platform diagnostics archive (archive process did not exclude the sparse file */var/log/lastlog*).
- Fixed processing of out-of-order TCP packets as well as processing of large TCP headers in Passive-Tap mode.
- TCP FIN packets were not processed in the correct order in inline modes, resulting in TCP queue processing timeouts.
- When displaying SSL session log entry details the UI now checks for the availability of certificate information; previous releases would have triggered an exception in the UI. The same updated logic is also applied to the fingerprint calculation on unsupported certificate key types.
- The in-memory X.509 caches are now limited in size to prevent the OOM killer from terminating the data-plane. The issue used to manifest itself when a large number of unique X.509 certificates were detected by the Sourcefire SSL appliance.
- Wild cards ('*' character) in X.509 subject fields are now treated as characters rather than wild cards in the policy engine. The rules in the policy may still use wild card characters. As an example: this fix allows the user to set up a rule to match the following CN: "cdn.*.livefilestore.com"
- TLS sessions with unsupported TLS extensions are now classified as undecryptable. Refer to See Section 2.2, *Important Information,* for more details.
- The UI now allows the user to reset the hostname by entering an empty value, which then translates into "localhost.localdomain" in the configuration.
- The UI webserver would sporadically reject file uploads with a "502" error because of the size of the HTTP header; the allowed header size was increased to resolve the issue.
- Fixed handling of TCP retransmits while decrypting certain cipher-suites (using block ciphers, for example, AES-CBC, 3DES-CBC), in the process fixing various types of TCP queue processing timeouts. The issue was especially prevalent when deploying the Sourcefire SSL appliance downstream from a F5 load-balance appliance.
- Process TLS CertificateStatus handshake messages; not processing those messages resulted in breaking certain browser page elements (such as twimg.com when connecting to Twitter).

- Allow setting the "Catch All Action" on rulesets; this was broken in version 3.6.3.
- Remove the X.509 Subject Key Identifier when applying "Decrypt (Resign Certificate)" and "Replace Key Only" actions to prevent invalid certificate errors in browsers.
- Empty user-defined policy lists used in rulesets no longer invalidate the rule referencing the list.
- Self-signed X.509 certificates seen on the wire had an erroneous validation status of both "Self-signed" *and* "Invalid Issuer".
- The IP header check logic was changed to allow fragments with the don't fragment (DF) bit set; those packets used to be discarded.
- Fixed issue when loading the UI in recent versions of the Chrome browser.
- When using user-defined PKI lists in rules and the list name has a specific length then the list would be ignored and would default to all entries of that specific type of PKI item.

2.5 Known Issues

- First-time boot may take up to 5 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 See Section 2.2, *Important Information,* 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 Sourcefire 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 Sourcefire 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 Blue Coat 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 See Section 2.2, *Important Information,* for more details.
- The Sourcefire SSL Appliance SSL2000 and SSL8200 models will try booting off of a USB stick if inserted into the front USB port.
- Deactivating an Active Inline segment may cause some packets to be received and retransmitted 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 Sourcefire 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 management features available on the web interfaces do not support IPv6 addresses.
- 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. Refer to See Section 2.2, *Important Information,* for more details.
- All platform configuration changes require rebooting the Sourcefire SSL appliance in order 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. The front panel LCD can be used 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 Sourcefire SSL appliance is rebooted.
- SSL session log entries for sessions using DSA cipher suites do not show public key fingerprints in detailed information.

- OCSP is not supported for server certificate validation. Only manually loaded CRLs can be used.
- 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 Sourcefire 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 device (for example, IPS) 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 device (e.g., IDS) 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 only an issue for 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 a Sourcefire SSL appliance recovers from an overload condition it may flag some SSL sessions with the "Invalid cryptographic response" error code

2.6 External CA Certificates Added in 3.7.0

The following X.509 CA certificates have been added since the 3.6.3 release:

- ADOCA02, GOV, DoD, PKI, CAs
- ANF Global Root CA, ANF Autoridad de Certificacion, ANF Clase 1 CA

- ApplicationCA2 Root, Japanese Government, GPKI
- Autoridad Certificadora Raíz Nacional de Uruguay, AGESIC
- Autoridad de Certificacion Raiz del Estado Venezolano, Sistema Nacional de Certificacion Electronica, Superintendencia de Servicios de Certificacion Electronica [3]
- CA DATEV BT 03, DATEV eG
- CA DATEV INT 03, DATEV eG
- CA DATEV STD 03, DATEV eG
- CA Disig Root R1, Disig a.s.
- CA Disig Root R2, Disig a.s.
- CA 沃通根证书, WoSign CA Limited
- Certification Authority of WoSign, WoSign CA Limited
- Certinomis - Root CA, Certinomis, 0002 433998903
- COMODO SSL CA 2, COMODO CA Limited
- DigiCert Assured ID Root G2, DigiCert Inc, www.digicert.com
- DigiCert Assured ID Root G3, DigiCert Inc, www.digicert.com
- DigiCert Global Root G2, DigiCert Inc, www.digicert.com
- DigiCert Global Root G3, DigiCert Inc, www.digicert.com
- DigiCert High Assurance EV CA-1, DigiCert Inc, www.digicert.com [2]
- DigiCert Trusted Root G4, DigiCert Inc, www.digicert.com
- E-GUVEN Kok Elektronik Sertifika Hizmet Saglayicisi S2, Elektronik Bilgi Guvenligi A.S.
- E-GUVEN Kok Elektronik Sertifika Hizmet Saglayicisi S3, Elektronik Bilgi Guvenligi A.S.
- E-Tugra Certification Authority, E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri AŞ., E-Tugra Sertifikasyon Merkezi
- Entrust Certification Authority - L1C, Entrust, Inc., www.entrust.net/rpa is incorporated by reference, (c) 2009 Entrust, Inc. [2]
- Entrust Root Certification Authority - EC1, Entrust, Inc., See www.entrust.net/legal-terms, (c) 2012 Entrust, Inc. - for authorized use only
- GeoTrust SSL CA - G2, GeoTrust Inc.
- GlobalSign, GlobalSign, GlobalSign ECC Root CA - R4
- GlobalSign, GlobalSign, GlobalSign ECC Root CA - R5
- Google Internet Authority G2, Google Inc
- Government Root Certification Authority [2]
- JCAN Root CA1, JIPDEC, JCAN Root CA1
- LAWtrust Root Certification Authority 2048, LAWtrust, LAW Trusted Third Party Services PTY Ltd.
- National Center for Digital Certification, Saudi National Root CA

- OATI WebCARES Root CA, Open Access Technology International Inc
- PSCProcert, Sistema Nacional de Certificacion Electronica, Proveedor de Certificados PROCERT
- QuoVadis Root CA 1 G3, QuoVadis Limited
- QuoVadis Root CA 2 G3, QuoVadis Limited
- QuoVadis Root CA 3 G3, QuoVadis Limited
- Signet Root CA, Telekomunikacja Polska S.A., Signet Certification Authority
- SSC GDL CA Root B, Skaitmeninio sertifikavimo centras, CA ROOT Services
- Staat der Nederlanden EV Root CA, Staat der Nederlanden
- Swisscom Root EV CA 2, Swisscom, Digital Certificate Services
- Symantec Class 1 Public Primary Certification Authority - G4, Symantec Corporation, Symantec Trust Network
- Symantec Class 1 Public Primary Certification Authority - G6, Symantec Corporation, Symantec Trust Network
- Symantec Class 2 Public Primary Certification Authority - G4, Symantec Corporation, Symantec Trust Network
- Symantec Class 2 Public Primary Certification Authority - G6, Symantec Corporation, Symantec Trust Network
- Symantec Class 3 Public Primary Certification Authority - G4, Symantec Corporation, Symantec Trust Network
- Symantec Class 3 Public Primary Certification Authority - G6, Symantec Corporation, Symantec Trust Network
- SZAFIR ROOT CA, Krajowa Izba Rozliczeniowa S.A.
- T-TeleSec GlobalRoot Class 2, T-Systems Enterprise Services GmbH, T-Systems Trust Center
- TM Applied Business Root Certificate, TM, TM Applied Business Certification Authority
- TWCA Global Root CA, TAIWAN-CA, Root CA
- VeriSign Class 3 Extended Validation SSL SGC CA, VeriSign, Inc., VeriSign Trust Network, Terms of use at https://www.verisign.com/rpa (c)06 [2]
- WellsSecure Public Root Certification Authority 01 G2, Wells Fargo WellsSecure, Wells Fargo Bank NA

3. Upgrading Sourcefire SSL Appliances from Version 3.7.1-70 to Version 3.7.1-71

3.1 Update Description

This software release for the SSL1500, SSL2000, and SSL8200 systems is a patch release which addresses the HeartBleed exploit, protecting against it for SSL traffic passing through and inspected by the Sourcefire SSL appliance. This patch allows you to protect internal servers and prevent vulnerable client systems from attack even if they visit a malicious SSL server.

The file associated with this patch release is:

- sslv-3.7.1-71-oem.patch

The patch upgrade mechanisms described below can be applied to any system that is running version 3.7.1-70 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 rescue image, and will revert to version 3.7.1-70. At that point you will need to re-apply the patch.

3.1.1 Applying the Patch

The Sourcefire SSL appliance must be running the version 3.7.1-70 software to use this patch. If necessary, upgrade to version 3.7.1-70 before applying version 3.7.1-71.

To apply the patch access the **Platform > Update** menu option on the WebUI, then select the sslv-3.7.1-71-oem.patch file, and click OK.

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

3.1.2 HeartBleed Overview

HeartBleed is a vulnerability in certain versions of the OpenSSL software stack that was made public on April 7th, 2014. The HeartBleed exploit relies on an error in the operation of a new TLS feature called TLS Heartbeat; the message is designed to allow an SSL stack to verify that the remote SSL stack it is communicating with is working correctly. Think of it as similar to a TCP Ping message; the TLS heartbeat message is send from one SSL device to another over an active TCP connection that is carrying a TLS session, and the recipient must turn the message around and send it back to the originator, so that the originator knows that the TLS connection is functioning correctly.

When the originator sends a TLS heartbeat message, it can include data in the message, and the recipient should return that data in the response that it sends back. The format includes a size field indicating how much data is included in the message, and includes this number as part of the message. The exploit is that if a TLS heartbeat message claims to contain 64 kb of data in the size field, but only includes 1 byte of actual data, this will not be flagged as an error.

The recipient of such a malformed message will trust the size field, and will generate a response that has the size field set to 64 kb and that contains 64 kb of data, not the original 1 byte included by the sender. The additional data is random data from memory accessible to the recipient SSL software. This causes the leakage of data from the recipient back to the sender and creates the security risk.

TLS heartbeat messages can be sent at any point during an SSL session, including during the SSL handshake, and they can be sent as many times as the originator wants to. It is important to note that use of the TLS heartbeat is symmetrical, meaning it can be sent by either the client or the server involved in an SSL connection. The problem is not restricted to servers. A maliciously crafted SSL server could use the HeartBleed exploit to read memory from clients connecting to it if the client was running a vulnerable version of OpenSSL. While patching vulnerable servers can be done fairly quickly and indeed for the major services is already complete, updating vulnerable client systems will take much longer and in some cases may not even be possible.

Protecting the Sourcefire SSL Appliance

A Sourcefire SSL appliance running v3.7.0-68 software was vulnerable to the HeartBleed exploit for SSL traffic to its management interface; there was NO vulnerability for SSL traffic that was passing through and being inspected by the appliance. As v3.7.0-68 was only released on April 3rd, there were very few systems running this software when the HeartBleed vulnerability was announced on April 7th. Blue Coat released a patch (v3.7.0-69) on April 8th, which removed the vulnerability for SSL traffic to the management port on the Sourcefire SSL appliance, and on April 15th a maintenance release (v3.7.1-70) was released that incorporated the patch and replaces all v3.7.0 software versions.

Protecting the Enterprise

While the Sourcefire SSL appliance is no longer vulnerable to HeartBleed, an Enterprise network may still have vulnerable SSL servers and SSL client systems that need protection. A Sourcefire SSL appliance running the sslv-3.7.1-71-oem.patch can supply that protection.

If the HeartBleed exploit occurs on an SSL flow that the Sourcefire SSL appliance is inspecting, with the new software feature provided in v3.7.1-71, the exploit will be detected, the flow terminated, and the event logged. This prevents the HeartBleed exploit from reaching the destination system and provides details on all attempted exploits, including details of the system that originated the exploit. Details of the exploit are stored in the SSL Session Log, and log messages are sent periodically to the system log if exploits are occurring.

It is important to note that the Sourcefire SSL appliance will detect the attack as long as we are inspecting the session, even if it occurs *after* the SSL session has become encrypted. While there are pattern matching solutions that can detect the exploit by comparing the TLS heartbeat sent by the originator and the TLS heartbeat returned by the destination which can work when the flow is encrypted, they require significantly more processing, and can only block the message coming back from the destination rather than preventing the exploit reaching the destination.

3.2 Resolved Issues

- Resolved a memory leak in the SSL intercept engine. The main symptom was lockup in one or more processing threads, resulting in no SSL sessions being inspected. In the worst case scenario, the data-plane process would crash and restart. The symptoms manifested in scenarios where large number of unique X.509 certificates were seen on the wire.

4. Technical Support

To obtain additional information or to provide feedback, please email support@sourcefire.com or contact the nearest Sourcefire technical support representative.

Visit https://support.sourcefire.com to download the latest documentation and software, access the knowledge base, or log a support ticket.