riverbed

RIVERBED PRODUCT RELEASE NOTES

PRODUCT: STEELHEAD CX

RELEASE DATE: 16-AUGUST-2023

VERSION: 9.14.2b

CONTENTS

1. SteelHead Version 9.14.2b
2. SteelHead Version 9.14.2a
3. SteelHead Version 9.14.2
4. SteelHead Version 9.14.1a
5. SteelHead Version 9.14.1
6. Known Issues
7. Upgrading RiOS Software Version
8. SteelCentral Controller for SteelHead Software Requirements
9. Hardware and Software Requirements
10. WinSec Controller for Steelhead Software Requirements
11. Contacting Riverbed Support

riverbed

1) SteelHead Version 9.14.2b

a) NEW FEATURES

No New Features in version 9.14.2b

b) FIXED PROBLEMS

- **STEELHEAD-17369** Symptom: With some traffic patterns, low throughput/traffic stoppage is seen due to TCP Zero Window on the outer channel.
  Condition: This issue can occur on 1-Gbps in-path interfaces, and only when VLAN tags are configured for the interface. This issue was introduced in release 9.14.1.

- **STEELHEAD-17003** Symptom: The router/switch EtherChannel interface goes down due to LACP packets being black-holed by a SteelHead.
  Condition: This issue occurs on the 4 x 10 Gbps and 2 x 40 Gbps in-path interfaces, and was introduced in release 9.14.1.

- **STEELHEAD-16910** Symptom: Excessive pause frames may be transmitted from the SteelHead appliance.
  Condition: This issue occurs in certain traffic situations on the 4x10Gbps and 2x40Gbps in-path interface cards especially on 7080B030 devices that do not have a QAT offload card, or 5080, 7080B010 and 7080B020 devices running older versions that do not take advantage of the on-board QAT offload functionality (9.12.x and earlier).

riverbed

2) SteelHead Version 9.14.2a

a) NEW FEATURES

No New Features in version 9.14.2a

b) FIXED PROBLEMS

- **STEELHEAD-17803** Symptom: NetFlow export may not function correctly. Condition: This issue occurs after upgrading to release 9.14.2.

- **STEELHEAD-17551** Symptom: An optimization service crash may occur.
  Condition: This issue occurs when the Adaptive Optimization feature is used for an extended period, and the internal list of hostnames reaches capacity (default: 5000). The Adaptive Optimization feature is disabled by default, and there is no risk when the feature is disabled. It is only an issue when the feature is enabled (*protocol profiler enable*) and the internal list is full. You can find the number of hostnames stored by generating a memory-dump file (included in a sysdump) and looking for the "Dumping Profiler" section. The first line shows the number of hostname entries. The Adaptive Optimization feature was introduced in 9.14.1. This issue does not affect that version.

- **STEELHEAD-18114** Symptom: Traffic generated from hosts with IPv6 and IPv4 addresses configured may create additional traffic logs.
  Condition: If a host is configured with IPv6 and IPv4 addresses, the traffic log may reflect the traffic multiple times under each IP class.

riverbed

3) SteelHead Version 9.14.2

a) NEW FEATURES

- **Domain-Independent SteelHead – Kerberos Optimization**
  We have added the capability to perform SMB optimization without domain join on the SteelHead.
- **SMB: Support Windows 11 and Windows Server 2022 Combination**
- **User Defined Routing (UDR) Deployment Option for Azure Cloud**
- **Failover Options with UDR**
- **TLS Adaptive Optimization improvements**
- **BMC version 21 is available for xx80. Includes improved logging**

b) FIXED PROBLEMS

- **STEELHEAD-17137** {{Details:}} OpenSSL version 1.1.1q on SteelHead is affected by CVE2023-0286 vulnerability. {{Fix:}} Components using this OpenSSL version on SteelHead are upgraded to version 1.1.1t with the fix to mitigate this vulnerability.
  {{Recommendation}}: Upgrade to a RiOS version with the fix.

- **STEELHEAD-17134** {{Details:}} OpenSSL version 1.0.2o on SteelHead is affected by CVE2023-0286 vulnerability. {{Fix: }} Components using this OpenSSL version on SteelHead are patched with the fix to mitigate this vulnerability. {{Recommendation}}: Upgrade to a RiOS version with the fix.

- **STEELHEAD-13797** Symptom: An SMB connection is not optimized between a Windows 11 client and Windows 2022 server.
  Condition: This issue is seen only with combination of Windows 11 client and Windows 2022 server. NOTE: WINDOWS 2022 IS NOT QUALIFIED FOR SMB OPTIMIZATION.

riverbed

- **STEELHEAD-16869** Symptom: SSH connections are refused for FIPS-enabled SteelHeads. Condition: This issue was introduced in releases 9.12.2b and 9.14.1.

- **STEELHEAD-16847** Some internal changes have made a slight increase in per connection memory use, when optimizing TLS connections, that may impact the connection capacity of older appliances. Although there is no impact expected during normal usage, improvements were made in the fix release in this area.

- **STEELHEAD-16735** Symptom: A client with a misconfigured CA trust can cause bypass affecting other clients.
  Condition: The TLS blade behavior was tuned so certificate trust errors generated by a client would only result in bypassing that specific client. Without this fix it is possible a single misconfigured client could cause widespread bypass of a server.

- **STEELHEAD-16632** Symptom: An optimization service crash can occur.
  Condition: The crash can occur when TLS blade optimized connections are disconnected.

- **STEELHEAD-16583** {{Details:}} The default configuration of the Kerberos protocol is affected by these vulnerabilities: CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. {{Fix: }} Added AES encryption type to default Kerberos protocol configuration to mitigate these vulnerabilities. {{Recommendation}}: Upgrade to a RiOS version with the fix.

- **STEELHEAD-16532** Symptom: “Reset Connection” in SteelHead’s web user interface fails with error message “Command execution failed” and the optimized connection is not reset. The script that resets the optimized connection fails to execute because it is not able to load the required shared libraries. The associated warning is logged:
  {noformat}[mgmtd.WARNING]: Exit with code 127 from /opt/rbt/bin/tcpctl{noformat}
  Condition: This issue occurs when a user resets an optimized connection from the Current Connections report in SteelHead's web user interface. With this fix the tcpctl script

correctly loads the necessary shared libraries to successfully reset an optimized connection.

- **STEELHEAD-16516** Symptom: On SteelHead-v with the ESXi platform, the ring buffers cannot be changed using the CLI commands.
  Condition: On the ESXi platform, modifying ring buffer size is not allowed in the mgmtd module. Added ring buffer modification support for the vmxnet3 driver in release 9.14.2 and later.

- **STEELHEAD-16325** Symptom: A system fault may occur when performing DNS lookup. Condition: This issue occurs due to a race condition and single thread getting blocked.

- **STEELHEAD-16324** Symptom: A policy push with a self-signed web certificate fails with this error: {noformat}Certificate chain verification failed: self signed certificate.{noformat}
  Condition: This issue occurs when the policy is pushed with a self-signed web certificate.

- **STEELHEAD-16319** Symptom: The *show peer ip ** CLI command displays incorrect output. Condition: When the *show peer ip ** command is used with an IP address not associated with a peer, the response shows it is connected. Results are correct for IPs associated with peers.

- **STEELHEAD-16291** Symptom: Peering Mode Client Authentication does not work with RSA key exchange in release 9.14.1.
  Condition: In RiOS 9.14.1, TLS client authentication will fail if using the SteelHead peering certificate (aka Peering Mode) and the selected cipher is using RSA key exchange. This issue only affects TLS v1.2 connections (which rarely use RSA key exchange).

- **STEELHEAD-16163** Symptom: Domain authentication for a child domain fails with a “Wrong Realm. Unable to reach LDAP server” replication error.

Condition: This issue occurs when a replication user with a wildcard domain or parent domain is configured.

- **STEELHEAD-16095** Symptom: On the SteelHead CX5080 model, the IP address is not persistent on the BMC port.
  Condition: This is caused by BMC firmware issue.

- **STEELHEAD-16074** Symptom: Optimizable client authentication connections are not being optimized.
  Condition: Certain web browsers (such as Chrome/Edge) will terminate connections when a client certificate is requested during a TLS handshake, and reopen a second follow-on connection at a higher security level to complete the handshake. These follow-on connections to complete the client authentication are not optimized properly.

- **STEELHEAD-16070** Symptom: Optimizable client authentication connections are not being optimized.
  Condition: Certain web browsers (such as Chrome/Edge) will terminate connections when a client certificate is requested during a TLS handshake, and reopen a second follow-on connection at a higher security level to complete the handshake. These follow-on connections to complete the client authentication are not optimized properly.

- **STEELHEAD-15989** * Updated the allowed KexAlgorithms supported by the SSH server and client on the SteelHead to remove weak algorithms. The KexAlgorithms list is now limited to these algorithms: curve25519-sha256 curve25519-sha256@libssh.org diffiehellmangroup-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellmangroup18sha512 diffie-hellman-group14-sha256

- **STEELHEAD-15845** Fixed an issue where the VCX installation script was not allocating enough CPU and RAM resources to Virtual SteelHeads VCX30, VCX40, and VCX50. The

installation script will now allocate the resources required per spec: [https://www.riverbed.com/sites/default/files/file/2023-02/steelhead-cxspecsheet.pdf|https://www.riverbed.com/sites/default/files/file/2023-02/steelheadcxspecsheet.pdf]

- **STEELHEAD-15605** Symptom: On SteelHead, the *web-proxy ssl-domain <domain> include-san* CLI command does not work with wildcard domains.
  Condition: This issue occurs because input is not processed for wildcard domains.

- **STEELHEAD-15494** Symptom: SteelHead shuts down in the AWS cloud.
  Condition: This issue occurs when the system clock goes out of sync and the DHCP lease expires.

- **STEELHEAD-15275** Symptom: An RBM user with in-path rule read permission cannot see the in-path rule details.
  Condition: This issue has been fixed.

- **STEELHEAD-14832** Symptom: The yarder_rbt process cannot start. It keeps exiting with this error: {{[yarder.core.ERROR] No row was found for one() Traceback (most recent call last): File "/usr/lib/python2.7/site-packages/ljcore/yarder/host/yarder.py", line 284, in host_main File "/usr/lib/python2.7/site-package s/ljcore/yarder/host/yarder.py", line 446, in start File "/usr/lib/python2.7/sitepackages/ljcore/yarder/host/service_module.py", line 432, in startup File "/usr/lib/python2.7/site-packages/lumberjack_svc_appflow/main.py", line 45, in startup
  File "/usr/lib/python2. 7/site-packages/lumberjack_svc_appflow/lib/tildriver/til_events.py", line 188, in read_initial_config File "/usr/lib/python2.7/site-packages/lumberjack_svc_appflow/globals/utils.py", line 581, in is_fec_enabled File "/usr/lib/python2.7/site-packages/lumberjack_svc_app flow/globals/utils.py", line 52, in

get_global_config File "/usr/lib64/python2.7/site-packages/sqlalchemy/orm/query.py", line 2355, in one NoResultFound: No row was found for one()}}
Condition: This issue occurs when QoS is configured before 8.6.0 (Maui) and STEELHEAD is getting upgraded from there to 9.12.2 (or any version in between).

- **STEELHEAD-14583** Symptom: The Azure Cloud Accelerator License page shows incorrect bandwidth and connection limit.
  Condition: This issue occurs because the system specification is not updated based on license configuration.

- **STEELHEAD-14469** Symptom: Under certain conditions, the output for *show peers onlineonly* command includes peers that are no longer online. This issue affects the summary as well, showing an incorrect number of connected appliances.
  Condition: The problem is limited to reporting and does not affect operation. The issue usually occurs when a server-side SteelHead peers with many Client Accelerators that are assigned IP addresses dynamically.

- **STEELHEAD-14413** {{Details:}} The Expat library version on SteelHead is affected by the CVE2022-23852 vulnerability. {{Fix: }} The Expat library version on SteelHead is patched with the fix to mitigate this vulnerability. {{Recommendation}}: Upgrade to a RiOS version with the fix.

- **STEELHEAD-14253** Symptom: Rebooting the appliance by pressing the power button isn't explicitly logged in various outputs, such as the *show reboot reasons* output. Condition: This issue affects the x80 and xx80 appliances that are running a BMC version earlier than v21. A RiOS upgrade does not necessarily upgrade the BMC. Contact support for instructions on updating the BMC.

riverbed

- **STEELHEAD-13351** Symptom: When updating the Current Connections Page with several thousand connections, a system fault may be rarely seen.
  Condition: This issue occurs due to a race condition and a missing null check.

- **STEELHEAD-10421** {{Details:}} A cross-site scripting vulnerability exists in the SteelHead UI web pages (Certificate Authorities). Importing a certificate with script data enables the cross-site scripting vulnerability in the appliance. {{Fix:}} Added conditions to check for script data in certificate content and remove the same from the certificate.
  {{Recommendation}}: Upgrade to a RiOS version with the fix.

- **STEELHEAD-9844** Symptom: Appliance reboots due the power button being pressed aren't explicitly logged in various outputs, such as the "show reboot reasons" output.
  Condition: This issue currently affects the x80 appliances. For appliances running updated CPLD and BMC versions, some log outputs will show the power button as a reboot reason.

4) SteelHead Version 9.14.1a

a) NEW FEATURES

No New Features available in version 9.14.1a

b) FIXED PROBLEMS

- **STEELHEAD-17010** Updated the allowed KexAlgorithms supported by the SSH server and client on the SteelHead to remove weak algorithms and readded secure algorithms. The KexAlgorithms list is now limited to these algorithms: diffie-hellmangroupexchangesha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512,

diffiehellmangroup14sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdhsha2nistp521.

- **STEELHEAD-16869** Symptom: SSH connections are refused for FIPS-enabled SteelHeads. Condition: This issue was introduced in releases 9.12.2b and 9.14.1.

- **STEELHEAD-16278** Symptom: On CX580, CX780, and CX3080 models, a port down on the SteelHead does not bring down the remote appliance port.
  Condition: This issue occurs when a driver upgrade causes a change in functionality.
- **STEELHEAD-16231** Symptom: Cannot configure speed and duplex for in-path LAN and WAN interfaces. Only “auto” is available as a configurable option.
  Condition: This issue is seen on all in-path LAN and WAN interfaces.

- **STEELHEAD-16163** Symptom: Domain authentication for a child domain fails with a “Wrong Realm. Unable to reach LDAP server” replication error.
  Condition: This issue occurs when a replication user with a wildcard domain or parent domain is configured.

- **STEELHEAD-16074** Symptom: Optimizable client authentication connections are not being optimized.
  Condition: Certain web browsers (such as Chrome/Edge) will terminate connections when a client certificate is requested during a TLS handshake, and reopen a second follow-on connection at a higher security level to complete the handshake. These follow-on connections to complete the client authentication are not optimized properly.

- **STEELHEAD-15989** Updated the allowed KexAlgorithms supported by the SSH server and client on the SteelHead to remove weak algorithms. The KexAlgorithms list is now limited to these algorithms: curve25519-sha256 curve25519-sha256@libssh.org diffiehellmangroup-exchange-sha256 diffie-hellman-group16-sha512 diffiehellmangroup18sha512 diffie-hellman-group14-sha256

- **STEELHEAD-15494** Symptom: SteelHead shuts down in the AWS cloud.
  Condition: This issue occurs when the system clock goes out of sync and the DHCP lease expires.

5) SteelHead Version 9.14.1

Notices:

TLS on version 9.14.1 SteelHeads and later interoperates with peers where TLS optimization is enabled. TLS optimization was first introduced in version 9.10.1 SteelHeads and Client Accelerator 6.3.1. Connections from peers running older versions automatically are passed through. TLS optimization supports features such as SSL Simplification and TLS v1.3 protocol. SSL Simplification refers to deployments where the Client Accelerator automatically provides certificates and brokers access to client certificates for client-authenticated connections.

See KB article https://supportkb.riverbed.com/support/index?page=content&id=S36609 for details.

Active Directory Integrated Mode (Windows 2008 and later)" is deprecated, and only "Kerberos Authentication" and "NTLM Authentication" are available. See KB article https://supportkb.riverbed.com/support/index?page=content&id=S35945 for details.

FIPS is not supported in this version.

riverbed

a) NEW FEATURES

Performance Improvements

Introduce Quick Assist Technology (QAT) Compression to Lower Model xx80 Appliances

The QAT card is currently only utilized in the 7080B030 models and not in B010 and B020 models.

With SteelHead 9.14.1, QAT Compression will be available in B010 and B020.

Benefit: Customers are seeking higher throughput for lower-end appliances as available bandwidth is improving. With this improvement, Compression improved by 50% and CPU utilization decreased by 40%

Filtering Out Low-Value Secure Socket Layer (SSL) traffic with Adaptive Optimization (formerly called host profiling)

Adaptive Optimization monitors TLS servers and can automatically prioritize which traffic to optimize. This is particularly important as SSL Simplification opens access to thousands of new servers and helps ensure SteelHeads focus on the high-value traffic.

Benefit: Without this feature, customers using SSL Simplification do not have insight into which hosts are optimizing well. Customers are trying to optimize all the SSL traffic with SSL Simplification and can reach SteelHead throughput limits faster.

Security Improvements

Transport Layer Security (TLS) 1.3 Support

58% of the top 1000 websites are now using TLS 1.3, Currently, we downgrade to TLS 1.2. In this release, the scope of the work will be limited to the optimization service data path (TLS inner and outer blades and Sepia). We are not upgrading management interaction to TLS 1.3.

Benefit: As customers migrate to TLS 1.3, we need to allow our product to use TLS 1.3. TLS 1.3 is compatible with 9.14.1, 9.12.x, and 9.10x.

Add a Secure Attribute to the Session Cookies

The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of the cookie in cleartext. By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel. **Benefit:** This fix is necessary to avoid vulnerability when a security scan is done.

Replicate Common Name (CN) to Subject Alternative Name (SAN) Fields for Cert Generation

Chrome changed how it processes certificates and now looks at the SAN field. To adjust to this change, we made changes to certification generation.

Benefit: We now align with how Chrome handles certificates averting any customer issues.

Usability Improvements

Easily Delete Trusted Certificates of Authority (CAs) and Replace Them with the Latest CAs

We have made it easier to update trusted CA's on SteelHead appliances.

Benefit: With this feature, customers can update CAs easily. This leads to fewer SSL certificate errors and better security.

Benefit: With this feature, customers can update CAs easily. This leads to fewer SSL certificate errors and better security.

Allow Up To 10 Domain Join Logs

Benefit: This makes troubleshooting easier.

riverbed

Cloud Accelerator Improvements

New Platform Version Qualification (Azure)

With this release, we are recommending new platform images. In this 9.14.1 release, we are qualifying the D2s_v5, D4s_v5, D8s_v5, E16s_v5, and E32s_v5 series.

Benefit: Qualifying these can result in a cost savings to customers of 20% to 32% as these newer versions use Solid State Drives (SSDs) and are cheaper to deploy.

Other

Win2K8 Mode Read Only Domain Controller (RODC) Deprecation

This enhancement switches the domain join mode from NTLM RODC to Kerberos workstation.

Benefit: This will help customers who are facing issues because of security improvements made by Microsoft with the NTLM protocol (in January 2022). These changes are applicable for both 9.12.2a and 9.14.1.

Bios Upgrade for CX3080, CX780, and CX580 **Benefit:**

Consistency with SteelConnect

Compatibility Updates

- **Hyper-V VSH deployment qualification on Windows 2019 Server**
- **Client OS Qualification – SMB2/3 optimization**
  - **macOS11**
  - **macOS12**
- **Windows 11 – with NetApp/Isilon Qualification**

riverbed

b) FIXED PROBLEMS

- **STEELHEAD-12996** Symptom: State Moving UP from CPUSTATE_NORMAL to CPUSTATE_MEDIUM, Reason: 100% of Blocking threads above threshold 45%, cutoff is 50% of threads above threshold.
  Condition: A WinSec controller is configured but not used for many days. The CPU state goes back to normal when a replication request is sent to the controller.

- **STEELHEAD-12985** Symptom: RiOS fails to come back online after an optimization service crash.
  Condition: This issue occurs when RiOS fails to allocate the required number of hugepages at RiOS startup after a crash, and is observed on higher end models.

- **STEELHEAD-12978** Symptom: Management access may be slow or unreachable with potential impact to optimization performance.
  Condition: This issue occurs in release 9.10.0 and later when the kernel's TCP memory pool is under pressure due one or more of these conditions: * large number of connections * high WAN latency * high throughput For these conditions, the system may have a soft lockup, which makes the appliance unusable.

- **STEELHEAD-12956** Symptom: The connection identifier is displayed as a negative number in the log messages. In this example, the connection identifier is displayed as 1376701320 in the log message: {noformat} Mar 31 19:47:12 STEELHEAD sport[1111]: [test/test.WARN] -1376701320 {10.10.10.10:1234 20.20.20.20:443} {noformat} Condition: When the number of connections exceeds the maximum value of int32 (typical value is 2147483647), the connection identifier may be displayed as a negative value in the log messages. This is only a display issue. With the bug fix, the connection identifier is always displayed as a positive number in the range 1 to 4294967295.

riverbed

- **STEELHEAD-12942** Symptom: Kerberos replication failed with error NT_STATUS_INVALID_PARAMETER.
  Condition: A larger than usual request to the DC prevents the SteelHead from communicating to a DC. Use the *\[no] protocol domain-auth dcerpc max-xmit large* command to increase the request size.

- **STEELHEAD-12890** Symptom: On the client-side SteelHead, the following NOTICE level log message is reported when MAPI-over-HTTP connections fail to get peer affinity with the server-side SteelHead: {noformat} Did not get peer affinity for this MOH connection, killing splice.{noformat} When this happens, the optimization service may crash depending on the traffic.
  Condition: This issue occurs when latency optimization is enabled for MAPI-over-HTTP traffic and the client-side SteelHead fails to get peer affinity with the server-side SteelHead.

- **STEELHEAD-12645** Symptom: The ampersand (&) character is displaying as "&amp" in the GUI Dashboard where the MOTD is displayed.
  Condition: If the MOTD section of the configuration contains an ampersand (&) character, then it is incorrectly displayed in the GUI as "&amp."

- **STEELHEAD-12573** Release Note Summary: Apache upgraded to version 2.4.46.
  {{Details:}} Apache server version 2.4.27 has multiple security vulnerabilities in SteelHead 9.12.0. {{Fix: }} The RiOS 9.12.0 uses Apache version 2.4.51, which is higher than the recommended version. {{Recommendation}}: Upgrade to a RiOS version with the fix.

- **STEELHEAD-12040** Symptom: Inconsistent password parsing occurs between the *configuration fetch* and *image fetch* CLI commands.
  Condition: This issue occurs when a question mark (?) or a colon (:) character is used in the password.

- **STEELHEAD-12004** Symptom: An optimization service crash occurs with error Smb2::SecInfoMetadata::sec_info_cache_cleanup.
  Condition: This issue can occur while optimizing SMB2 connections.

- **STEELHEAD-11737** *Symptom:* Logs contain messages to this effect: {noformat}Oct 30 10:24:53 SteelHead kernel:INFO: task flush-259:0:1889 blocked for more than 120 seconds . Oct 30 10:24:53 SteelHead kernel: Tainted: P – ---------- 2.6.32 #1 Oct 30 10:24:53 SteelHead kernel:"echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables ... Oct 30 10:28:35 SteelHead statsd[18803]: [statsd.ERR]: lc_launch_exec(), proc_utils.c:951, bui ld (null): No such file or directory: Exec of /usr/sbin/rndc failed Oct 30 10:28:35 SteelHead statsd[18803]: [statsd.ERR]: lc_launch(), proc_utils.c:413, build (n ull): Forked process failed exec(), exiting Oct 30 10:28:35 SteelHead statsd[23028]: [statsd.ERR]: lc_launch_post_fork_parent(), proc_util s.c:670, build (null): Exec of /usr/sbin/rndc failed, error code -1 Oct 30 10:28:37 SteelHead kernel:EXT3-fs error (device nvme0n1p5): ext3_get_inode_loc: unable to read inode block - inode=204872, block=819208{noformat} *Condition:* This issue occurs on units that have Swissbit NVMe SSD running firmware SBR11010. *NOTE:* Upgrading to a fixed version does not by itself invoke the fix. Additional steps are required to invoke the fix. Contact Riverbed Support and reference STEELHEAD11737 to confirm a match for the bug and receive the fix instructions.

- **STEELHEAD-11568** Symptom: SMB connections are blacklisted with KRB authentication errors (KSTORE_KEY_NEW).
  Condition: When an SMB connection is attempted for a server name with the same prefix as that of an already-mapped server name, KRB authentication failures are seen, resulting in the connection being blacklisted.

- **STEELHEAD-11530** Symptom: An in-path LAN or WAN interface is down with "Detected Tx Unit Hang” noted in the system log.
  Condition: This issue affects the 580, 780, and 3080 appliances.

riverbed

- **STEELHEAD-11442** Symptom: High CPU alarms occur on the SteelHead CX 7070 appliance. Condition: This issue occurs on the SteelHead CX 7070 appliance when running release 9.9.0.b. SteelHeads that handle many long-lived connections can end up repeatedly looking for data to flush to disk. The rest period between checks is not being observed, causing high CPU alarms. No known problem results from this bug, besides CPU overuse.

- **STEELHEAD-11249** Symptom: An optimization service crash occurs.
  Condition: This issue can occur when optimizing signed SMB2 connections.

- **STEELHEAD-11241** Symptom: Replacing a web certificate with an internal CA-signed certificate fails with Internal Error (Unsupported scheme 'ldap'). Condition: This issue occurs in version 9.10.0.

- **STEELHEAD-11035** Symptom:. An optimization service crash occurs. Condition: This issue occurs during SMB2 traffic optimization.

- **STEELHEAD-10876** Symptom: An optimization service crash occurs with log messages such as "Not saving 401/407 response due to excessive memory use or mem AC." Crash is "PageHeap::New() grow heap failed."
  Condition: This issue occurs when SMB optimisations predominate the traffic mix. || || || || | | | | | | | |

- **STEELHEAD-10555** *Symptom:* Kerberos replication fails with error “Unable to obtain server key <SPN>” message and the SMB2/3 connections get blacklisted.
  Condition: The can occur with signed SMB2/3 traffic. The server side Steelhead randomly receives wrong SPN strings of the format “CIFS/SMA*/RVBD” in the Kerberos AP_REQ packets. The LDAP query from server side Steelhead to Domain Controller for this SPN lookup fails, resulting in error “Unable to obtain server key for RVBD\\SMA*/RVBD. Lookup failure. Unable to find machine account for SMA2071/RVBD”.

- **STEELHEAD-10503** Symptom: An in-path interface spontaneously goes down and does not come back up until the appliance is rebooted.
  Condition: This issue can occur on the 580, 780, and 3080 models.

- **STEELHEAD-10056** Symptom: An optimization service crash occurs with error “SIGSEGV in Smb2::safe_shared_ptr<Smb2::LeaseContext>.”
  Condition: This issue can occur when optimizing SMB2 traffic.

- **STEELHEAD-14154** Symptom: When parsing the STEELHEAD-MIB.txt file, syntax and import errors occur.
  Condition: This issue occurs when you try to monitor the device using SNMP but are unable to parse the STEELHEAD-MIB.txt file.

- **STEELHEAD-14090** Symptom: The optimization service may crash while optimizing MAPIover-HTTP requests with extended buffer packing.
  Condition: While optimizing MAPI-over-HTTP requests with extended buffer packing, a copy of the request data may be held by the optimization service until the MAPI-over-HTTP session context expires. When multiple MAPI-over-HTTP requests with extended buffer packing are optimized, it may lead to an optimization service crash due to out of memory. Optimization of each MAPI-over-HTTP request with extended buffer packing displays the following INFO level log message: {code:java}Bypassing an Execute request with extended buffer packing{code} When bypassing an Execute request with extended buffer packing, the above bug is fixed by releasing the memory held by the Execute request.

- **STEELHEAD-14056** Symptom: An optimization service crash can occur with message: Sport crash occurred "PageHeap::New() grow heap failed".
  Condition: This can occur when optimizing traffic through any of the latency optimization blades. Limit checks were added to accommodate over-buffering situations.

riverbed

- **STEELHEAD-14049** Symptom: With TLS optimization enabled, a connection may be passed through with the WARN level error message "Problem creating CommonConfig." Condition: This issue occurs after a SteelHead reboot when a custom secure vault password has been configured. The secure vault has not been unlocked.

- **STEELHEAD-13968** Symptom: SteelHead does not preserve the order of the dc-list given in the *domain settings dc-list* command. It sorts configured DC hosts in alphanumeric order. Condition: When hard coding the closest/fastest DCs in the dc-list using the *domain settings dc-list* command, the order does not get maintained. Instead, SteelHead picks the first DC after alphabetically sorting the dc-list, which might not be the closest/fastest DC as given in the input dc-list order.

- **STEELHEAD-13933** Symptom: All processing and third-party entities, including acquirers, processors, gateways, and service providers, must provide a TLS version 1.2 or later service offering by June 2018. All processing and third-party entities must cut over to a secure version of TLS (as defined by NIST) effective June 2018.
  Condition: TLS version 1.1 is disabled by default for the Interceptor and SteelHead UI. If required, TLS version 1.1 can be enabled using the *web ssl protocol tlsv1.1 enable* CLI command.

- **STEELHEAD-13897** Symptom: Unable to load or install a valid CA certificate with the CRL URI.
  Condition: This issue occurs when the URI is not accessible from SteelHead.

- **STEELHEAD-13873** Symptom: Logs indicate rapid connection attempts and failures by the Keystone transport. This continues until incoming connections stop or the issue that is preventing a successful transport connection is resolved.
  Condition: The Keystone transport connection, used when TLS is enabled, is requested based on an incoming connection, but the transport connection fails.

riverbed

- **STEELHEAD-13869** Release Note Summary: Apache version 2.4.46 has multiple security vulnerabilities.
  {{Details:}} Apache server version 2.4.46 has a couple of security vulnerabilities, which are CVE-2021-39275 and CVE-2021-34798. {{Recommendation: }} Upgrade the Apache version to 2.4.49 or later to mitigate these vulnerabilities. {{Fix}}: Upgraded the Apache version to the 2.4.51.

- **STEELHEAD-13638** Symptom: Windows 10 clients cannot rename or move files on SMB share.
  Condition: A software defect in SteelHead SMB latency optimization prevents some Windows 10 clients from renaming or moving files.

- **STEELHEAD-13611** Release Note Summary: Added HTTP Strict Transport Security (HSTS) response header.
  Symptom: An HTTP Strict Transport Security (HSTS) vulnerability exists. HSTS is missing from the HTTPS server.
  Condition: This issue occurs when a user tries to log in using HTTP instead of HTTPS.

- **STEELHEAD-13595** Symptom: There is an unexpected failure of process domhealthd, when using “auto configuration” to configured a replication account.
  Condition: This issue occurs during auto configuration of the replication account and the account doesn’t have sufficient privilege.

- **STEELHEAD-13594** Symptom: Debug logs on the server-side SteelHead show an error such as this: \[/keystone/core DEBUG] \{- -} \[Transport] Failed to find transport 1 to remove dup jobs Future client certificate operations on the server-side SteelHead may begin to fail immediately, which causes SSL optimization to fail for hosts that require client certificates.
  Condition: TLS blade is enabled and a client certificate is requested, but the operation times out.

- **STEELHEAD-13515** Symptom: The optimization service process fails with a stack trace.
  Condition: SteelHead crashes when it receives a malformed NTLM authentication message.

- **STEELHEAD-13482** Symptom: SMB latency optimization denies access to a file when the file's path differs only in the letter case.
  Condition: A file is accessed with a path that contains an alternate letter case than what is stored at the SMB server's share file system. SMB paths are case-preserving, but SMB latency optimization treats them as case-sensitive. This behavior is modified to match ASCII path names in a case-insensitive manner. If the path contains non-ASCII letters, the default behavior is to use case-sensitive comparison of path names. Use the *protocol smb2 caseless enable* command to change this behavior: NOTE: SMB latency optimization uses the ICU library to compare non-ASCII file paths, and the comparison of some paths might not match with the behavior of the SMB share's file system. For details, go to this Knowledge Base article: ?? [https://supportkb.riverbed.com/support/index?page=content&id=S28940|https://supportkb.riverbed.com/support/index?page=content&id=S28940]

- **STEELHEAD-13478** Symptom: In rare cases, a TLS handshake message may span more than one TLS record.
  Condition: The TLS blade has been updated to handle these TLS handshake records: Certificate, Certificate Request, Certificate Status.

- **STEELHEAD-13456** Symptom: The in-path rules "Hit Count" and "Last Hit Time" incorrectly read zero.
  Condition: These in-path rules remain zero even if hit.

- **STEELHEAD-13449** Symptom: A domain authentication alert is raised with an NT_STATUS_NO_LOGON_SERVERS error because a DC connection issue does not get cleared even after the DC connectivity is restored or new DCs are added to the domain.

Condition: Due to certain network conditions, discovering the domain controllers takes longer than the client specified timeout. The winbind process enters an inconstant state and fails to clear the alarm.

- **STEELHEAD-13265** Symptom: A domain authentication alert is raised with an NT_STATUS_NO_LOGON_SERVERS error because a DC connection issue does not get cleared even after DC connectivity is restored.
  Condition: When DC communication is unavailable for a prolonged period, winbindd marks the domain as offline and auth requests are not sent to the DCs until DC discovery finds the DC after a successful CLDAP request. Due to a software bug in the code, sometimes even when the DC discovery returns a valid DC with successful CLDAP, the connection to the DC is not attempted, leaving the domain in an offline state for a long time until winbind is restarted.

- **STEELHEAD-13249** Symptom: The second swap partition was not created, which could lead to unexpected performance impact.
  Condition: This issue was introduced in 9.12.0 for VCX40 - VCX110. Please note that to solve this issue, run a fixed version (9.12.1 or later) **and increase the management disk size.** (The specification is changed in 9.12.1 to accommodate this). Refer to KB article [https://supportkb.riverbed.com/support/index?page=content&id=S35294|https://supportkb.riverbed.com/support/index?page=content&id=S35294].

- **STEELHEAD-13153** Symptom: The web UI and CLI are nonresponsive with multiple “Timed out getting external query response from sport” errors in the system.
  Condition: This issue can occur with a high connection count, running a current connections report, and there is a flow collector configured with a hostname instead of an IP address.

- **STEELHEAD-13144** Symptom: The Kerberos key replication cache needs improvements to make it consistent for WinSec and Winbindd.

Condition: The Kerberos key replication cache efficiency is improved by keeping the cache of those keys that are more likely to be used in future. The SteelHead attempts to optimize client traffic that use older Kerberos keys if the server allows the use of such keys.

- **STEELHEAD-13134** Symptom: Packet drops are seen for NetFlow traffic. Condition: This issue occurs when Packet mode optimization is enabled.

- **STEELHEAD-15042** Symptom: The SteelHead domain leave operation gets stuck for 7 minutes 32 seconds if the primary DNS IP address is changed.
  Condition: Once SteelHead is in the domain joined state, if the primary DNS IP address is changed and the domain leave operation is triggered, the domain leave operation will get stuck for 7 minutes 32 seconds.

- **STEELHEAD-15033** Symptom: Cloud SteelHead Licensing (Cloud server and token application) is hidden in 9.12.2.
  Condition: This issue occurs in the AZUREVMCSH model.

- **STEELHEAD-14962** Symptom: The optimization service crashes.
  Condition: This can occur during data plane traffic, in a race condition accessing memory. This is observed in higher end models.

- **STEELHEAD-14834** Symptom: A connection reset occurs.
  Condition: Dialect number 0x2ff in the negotiate request causes the connection reset.

- **STEELHEAD-14818** Symptom: In certain deployment scenarios, application classification for SaaS Accelerator can generate a large number of DNS queries.
  Condition: This issue can occur if the classifications are attempted on ephemeral ports, which do not cache well. A new CLI command *\[no] service saas-accel acs limit enable*

has been added to restrict classification to the HTTPS port 443. This command is disabled by default.

- **STEELHEAD-14815** Release Note Summary: OpenSSL is updated with fix for CVE-20220778. Details: The current OpenSSL version, v1.0.2o, is affected by CVE-2022-0778. This causes an infinite loop in BN_mod_sqrt() reachable when parsing certificates. Recommendation: Upgrade to a version that contains this bug fix. Fix: Patched the OpenSSL package with the fix for CVE-2022-0778.

- **STEELHEAD-14814** Symptom: A Virtual Steelhead VCX30 is not given enough RAM to run properly.
  Condition: This issue occurs because the VCX30 allowed 2GB of RAM, even though it requires 4GB of RAM to run properly.

- **STEELHEAD-14619** Symptom: A log message now shows when an error occurs in the inner or outer connection of an optimized connection. Following is a sample error message without the fix for this bug: {code:java}sport[15973]: [splice/client.ERR] 2796182 {10.44.32.32:62823 10.10.10.10:80} Error while reading: Connection timed out{code} Condition: The above log message does not indicate if the error occurred in the inner or outer connection. The log message is updated to report this information. Following are sample log messages: {code:java}sport[15973]: [splice/client.ERR] 2796182 {10.44.32.32:62823 10.10.10.10:80} Error while reading from inner connection: Connection timed out sport[15973]: [splice/client.ERR] 2796182 {10.44.32.32:62823 10.10.10.10:80} Error while reading from outer connection: Connection timed out sport[15973]: [splice/client.ERR] 2796182 {10.44.32.32:62823 10.10.10.10:80} Error while writing to inner connection: Connection timed out sport[15973]: [splice/client.ERR] 2796182 {10.44.32.32:62823 10.10.10.10:80} Error while writing to outer connection: Connection timed out{code}

riverbed

- **STEELHEAD-14617** Symptom: Unhealthy threads and optimization service failure occur with multiple NFS stack traces with at least one of them pointing to pthread_mutex_lock. Condition: This issue occurs when there is a large number of NFS read requests.

- **STEELHEAD-14615** Symptom: SteelHead reboots unexpectedly with a kernel panic. Condition: This issue occurs when NSH enabled.

- **STEELHEAD-14592** Symptom: Performance issues occur when connections are optimized with the VCX-30.
  Condition: The memory limit for the optimization service is incorrectly configured, leading to a low-memory state in the codec flow control. The codec flow control does not increase the window size for the inner channel due to the low-memory state. This results in slowness even when the bandwidth reduction is good. The memory limits for the optimization service are correctly configured for the VCX-30 by this bug fix.

- **STEELHEAD-14572** Symptom: An optimization service failure may occur when SMB2 latency optimization is used.
  Condition: This issue occurs when using a directory that contains non-ASCII characters in filenames or a mix of ASCII and non-ASCII characters in filenames.

- **STEELHEAD-14477** Symptom: SteelHead reboots unexpectedly with a kernel panic. Condition: This issue occurs when NSH enabled.

- **STEELHEAD-14339** Symptom: An optimization service may can occur, and the following warning is logged: {{[socket.WARN] - {- -} cannot set O_NONBLOCK: Bad file descriptor}} Condition: This race condition can occur when a WinSec controller is used for domain authentication.

riverbed

- **STEELHEAD-14308** Symptom: It takes more than the usual time to configure a flow collector, and the flow collector prints info level logs "unable to send flow packet." Condition: This can occur when the flow collector host is unresolvable.

- **STEELHEAD-14287** Symptom: # Domain join from SteelHead devices display the error “Failed to join domain using ads: failed to verify domain membership after joining: The object name is not found.” # When SteelHead is already joined to the domain in Active Directory Integrated mode (Windows 2008 and later), it may report NT_STATUS_OBJECT_NAME_NOT_FOUND during the mutual authentication while SMB2/3 protocol sessions are intercepted.
  Condition: These issues are seen after the January 2022 security updates are applied on the domain controllers. |*Domain Controller OS version*|*January 2022 Updates*|*Outofband*| |Windows Server 2012|[5009586|https://support.microsoft.com/help/5009586] (Monthly Rollup)|[5010797|https://support.microsoft.com/help/5010797]| |Windows Server 2012 R2|[5009595|https://support.microsoft.com/help/5009595] (Security Update) [5009624|https://support.microsoft.com/help/5009624] (Monthly Rollup)|[5010794|https://support.microsoft.com/help/5010794]| |Windows Server 2016|[5009546|https://support.microsoft.com/help/5009546] (Security Update)|[5010790|https://support.microsoft.com/help/5010790]| |Windows Server 2019|[5009557|https://support.microsoft.com/help/5009557] (Security Update)|[5010791|https://support.microsoft.com/help/5010791]| |Windows Server 2022|[5009555|https://support.microsoft.com/help/5009555] (Security Update)|[5010796|https://support.microsoft.com/help/5010796]|

- **STEELHEAD-15717** Symptom: The optimization service might terminate unexpectedly. Condition: This issue occurs when a file is accessed over SMB2 share, the path to the file has non-ASCII characters, and the file is renamed to alter only the letter casing.

riverbed

- **STEELHEAD-15660** Symptom: High CPU is observed on an SCC.
  Condition: This is observed in 9.10.0 and later, and can occur after a policy push to an appliance.

- **STEELHEAD-15491** {{Details:}} Apache version 2.4.53 has multiple security vulnerabilities. These CVEs are fixed in Apache version 2.4.54: [https://nvd.nist.gov/vuln/detail/CVE-2022-26377|https://nvd.nist.gov/vuln/detail/CVE-2022-26377|smart-link] [https://nvd.nist.gov/vuln/detail/CVE-2022-28330|https://nvd.nist.gov/vuln/detail/CVE2022-28330|smart-link] [https://nvd.nist.gov/vuln/detail/CVE-2022-28614|https://nvd.nist.gov/vuln/detail/CVE-2022-28614|smart-link] [https://nvd.nist.gov/vuln/detail/CVE-2022-28615|https://nvd.nist.gov/vuln/detail/CVE2022-28615|smart-link] [https://nvd.nist.gov/vuln/detail/CVE-2022-29404|https://nvd.nist.gov/vuln/detail/CVE-2022-29404|smart-link] [https://nvd.nist.gov/vuln/detail/CVE-2022-30556|https://nvd.nist.gov/vuln/detail/CVE2022-30556|smart-link] [https://nvd.nist.gov/vuln/detail/CVE-2022-30522|https://nvd.nist.gov/vuln/detail/CVE-2022-30522|smart-link] [https://nvd.nist.gov/vuln/detail/CVE-2022-31813|https://nvd.nist.gov/vuln/detail/CVE2022-31813|smart-link] {{Recommendation:}} Upgrade the Apache version to 2.4.54 to mitigate these vulnerabilities. {{Fix}}: Upgraded the Apache version to 2.4.54.

- **STEELHEAD-15482** Symptom: The CLI command to enable and disable the SCPS feature gets reset to the default, and traffic going as RiOS+SCPS though the SCPS feature is disabled. Condition: This issue occurs after a reboot.

- **STEELHEAD-15327** Symptom: The maximum number of SYN retransmits is reset to the default value of 5.

Condition: This issue occurs when case latency detection is enabled and the appliance is rebooted.

- **STEELHEAD-15314** Symptom: A regular expression filter gives unexpected output. Condition: This issue occurs when applying a port number in the regular expression in the current connections page.

- **STEELHEAD-15310** Symptom: SNMP traps are missing for the asymmetric routing condition.

- **STEELHEAD-15306** Symptom: Site traffic can be blocked by SteelHeads that have peering trust misconfigured.
  Condition: This issue is limited to situations where latency optimization is enabled and connections are being initiated from both peer LANs. On the client SteelHead you will see repeated instances of this message: {noformat}[Jun 14 23:05:12 7283 3 /splice/client ERR] {10.5.148.132:38509 10.5.148.123:443} Error while writing: Broken pipe{noformat} You will not see this message: {noformat}[Jun 14 23:10:45 13842 0 /sslinnerchan/bypass_table WARN] {- -} Temporarily disabling interception of traffic for 10.5.148.123:443 - Misconfiguration of inner SSL security between client-side and server-side Steelhead appliances{noformat} On the server SteelHead you will see this message for each dropped connection almost immediately after the connection starts: {noformat}[Jun 14 23:05:03 8690 2 /sslinnerchan/server NOTICE] {10.5.148.132:38508 10.5.148.123:443} Dropping connection{noformat}

- **STEELHEAD-15130** Symptom: SteelHead-v on Nutanix bootup is delayed when no key is pressed during bootup.
  Condition: This issue occurs when SteelHead-v on Nutanix is manufactured or reloaded.

- **STEELHEAD-9927** Symptom: SteelHead optimization service fails as SteelHead runs out of memory.

Condition: An SMB client causes an optimization service process failure by repeatedly creating new sessions on a TCP connection.

- **STEELHEAD-9876** Symptom: An optimization service crash occurs. Condition: This issue can occur when optimizing SMB2.

- **STEELHEAD-9692** Symptom: An optimization service crash occurs due to a memory allocation failure.
  Condition: Memory is not managed appropriately for the resolving hostname.

- **STEELHEAD-9320** Symptom: America South Brazil East daylight saving time is not correct. Condition: This issue occurs when America South Brazil East daylight saving time is used and the time zone database is not updated.

- **STEELHEAD-8732** Symptom: Small packets (such as TCP ACK packets) are blackholed, leading to traffic interruptions.
  Condition: This issue occurs on small packets that are VLAN tagged. Only these interface cards are impacted: - 4x10G interface cards: NIC-1-010G-4SR-BP and NIC-1-010G-4LR-BP - 2x40G interface cards: NIC-1-040G-2SR4-BP and NIC-1-040G-2LR4-BP These cards are not impacted: - Any 1Gig interface - 2x10G interface cards: NIC-1-010G-2SR-BP and NIC1010G2LR-BP

- **STEELHEAD-8728** Symptom: NOTICE level log messages with “No entry for \[rpc xid=” from NFS (SunRPC) are seen in SteelHead logs.
  Condition: An NFS server is slow to respond.

- **STEELHEAD-8328** Symptom: An optimization service failure may occur along with "watcher: EventThread(worker) is not healthy" messages. Condition: This can occur when optimizing NFSv3 traffic.

- **STEELHEAD-7801** Symptom: CVE-2019-12456 double fetch in mpt3sas_ctl.c. Condition: Local DoS attack due to vulnerability from CVE-2019-12456 in mpt3sas_ctl.c.

- **STEELHEAD-7800** Release Note Summary: Kernel patches for CVE-2019-12378. {{Details:}} An issue was discovered in ip6_ra_control in net/ipv6/ipv6_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). RiOS uses the Linux kernel version that is prior to 5.1.5, and this vulnerability has impacted the current version. More information can be found here: [https://nvd.nist.gov/vuln/detail/CVE-2019-12378|https://nvd.nist.gov/vuln/detail/CVE2019-12378|smart-link] {{Fix: }} Patch the kernel with the fix for this vulnerability. {{Recommendation}}: Upgrade to a version with the fix.

- **STEELHEAD-7786** Release Note Summary: Kernel patches for CVE-2018-20836. {{Details:}} An issue was discovered in the Linux kernel before 4.20. There is a race condition in smp_task_timedout() and smp_task_done() in drivers/scsi/libsas/sas_expander.c, leading to a use-after-free. RiOS uses the Linux kernel version that is prior to 4.20, and this vulnerability has impacted the current version. More information can be found here: [https://nvd.nist.gov/vuln/detail/CVE201820836|https://nvd.nist.gov/vuln/detail/CVE2018-20836] {{Fix: }} The kernel has been patched with the fix. {{Recommendation}}: Upgrade to a RiOS version with the fix.

- **STEELHEAD-7785** Release Note Summary: Kernel patches for CVE-2019-11810. {{Details:}} An issue was discovered in the Linux kernel before 5.0.7. A NULL pointer dereference can occur when megasas_create_frame_pool() fails in megasas_alloc_cmds() in drivers/scsi/megaraid/megaraid_sas_base.c. This causes a Denial of Service related to a use-after-free. RiOS uses the Linux kernel version that is prior to 5.0.7, and this vulnerability has impacted the current version. More information can be found here:

[https://nvd.nist.gov/vuln/detail/CVE-2019-11810|https://nvd.nist.gov/vuln/detail/CVE2019-11810|smart-link] {{Fix: }} The kernel has been patched with the fix for this vulnerability. {{Recommendation}}: Upgrade to a RiOS version with the fix.

4) KNOWN ISSUES

- **STEELHEAD-16194** Symptom: SteelHead-v appliances on Hyper-V becomes inaccessible via CLI or web UI.
  Condition: This issue occurs when the SteelHead-v appliance is rebooted by configuring inpath interface with out-of-path and MTU is modified.

- **STEELHEAD-13384** Symptom: The second swap partition was not created, which could lead to unexpected performance impact.
  Condition: This issue was introduced in 9.12.0 for VCX40 - VCX110. Please note that to solve this issue, run a fixed version (9.12.1 or later) **and increase the management disk size.** (The specification is changed in 9.12.1 to accommodate this). Refer to KB article [https://supportkb.riverbed.com/support/index?page=content&id=S35294|https://supportkb.riverbed.com/support/index?page=content&id=S35294].

- **STEELHEAD-12288** Winsec Controller connectivity is not supported in environments with Path Selection

- **STEELHEAD-10658** Symptom: Optimized HTTPS/SSL 1.1 traffic is classified as HTTP traffic.
  Condition: This issue occurs only on HTTPS/SSL 1.1 traffic (not HTTP-2) where optimized traffic is classified as HTTP traffic, whereas pass-through is classified correctly as HTTPS/SSL.

- **STEELHEAD-6411** Symptom: The current connections report shows zero optimized connections.
  Condition: This issue occurs in some high-connection scenarios.

5) UPGRADING RIOS SOFTWARE VERSION

UPGRADING ALERT

- **9.2.0 Upgrade, Path Selection and QoS**: Operators must disable path selection and QoS in SteelHead 9.0.x or SteelHead 9.1.x prior to rebooting into SteelHead 9.2.0 and later versions, which uses new path identifiers. Go to Knowledge Base article S28250 for detailed instructions. Failure to follow this process can block pre-existing connections and render the SteelHead unreachable after the first SCC 9.2.0 Path Selection policy push.

- **Path Selection**: Upon upgrading a SteelHead from RiOS version 8.6.x or earlier to 9.0.0 and later, existing path selection rules are not automatically migrated. Go to Knowledge Base article S25533 for details.

- **QoS**: RiOS version 9.0.0 and later uses a completely new QoS management and syntax compared to RiOS version 8.6.x and earlier. Go to Knowledge Base article S25532 for details prior to upgrading to RiOS version 9.0.0 and later.

  Review the *SteelHead CX Installation and Configuration Guide* for information on upgrading the RiOS software version on SteelHead appliances. For Virtual SteelHeads, see the *Virtual SteelHead CX Installation Guide*. If running Cloud SteelHeads, see the *Riverbed Cloud Services User's Guide*.

riverbed

6) STEELCENTRAL CONTROLLER FOR STEELHEAD SOFTWARE REQUIREMENTS

SCC was formally known as Central Management Console (CMC). Review the SteelHead CX Installation and Configuration Guide for information on SCC compatibility.

7) WINSEC CONTROLLER FOR STEELHEAD SOFTWARE REQUIREMENTS

For WinSec Controller users, RIOS 9.12.1 and later requires WInSec to run a minimum of 1.1.0. WinSec should be upgraded first (1.1.0 is backward compatible with RIOS 9.12.0), before upgrading the Steelhead appliances. For later Steelhead releases, consult this section in later releases for any change in this requirement.

8) HARDWARE AND SOFTWARE REQUIREMENTS

Review the *SteelHead CX Installation and Configuration Guide f*or information on upgrading the RiOS software version on SteelHead appliances. For Virtual SteelHeads, see the *Virtual SteelHead CX Installation Guide.* If running Cloud SteelHeads, see the *Riverbed Cloud Services User's Guide.*

9) CONTACTING RIVERBED SUPPORT

Visit the Riverbed Support site to download software updates and documentation, browse our library of Knowledge Base articles and manage your account. To open a support case, choose one of the options below.

riverbed

Phone

Riverbed provides phone support at 1-888-RVBD-TAC (1-888-782-3822). Outside the U.S. dial +1 415 247 7381.

Online

You can also submit a support case online.

Email

Send email to support@riverbed.com. A member of the support team will reply as quickly as possible.