riverbed

RIVERBED PRODUCT RELEASE NOTES

PRODUCT: STEELHEAD CX

RELEASE DATE: 27-DECEMBER-2023

VERSION: 9.15.0

CONTENTS

riverbed

1) SteelHead Version 9.15.0

a) NEW FEATURES

Aimed at improving usability and compatibility, this release includes features relevant to the Federal space including support for IPv6 and Cisco Secure Group Tagging (SGT). The release also introduces support for new SMB 3.1.1 crypto algorithms (AES-GCM, AESCCM, AES-GMAC), DISKO support for short domain names, and DISKO performance improvements. In addition, security improvements to the SteelHead Certificate Signing Service provide an easy path for TLS/SSL optimization without the need for an agent.

b) Ipv6 Support

Riverbed is continuing its efforts to make its products fully compatible with Ipv6. Reference the following KB article to understand acceleration product Ipv6 support: https://supportkb.riverbed.com/support/index?page=content&id=S38049&actp=search

c) FIXED PROBLEMS

- **STEELHEAD-20056** Symptom: Outlook connections do not work reliably with the "Strip Compression" optimization.
  Condition: Certain applications and servers have always had problems with the "Strip Compression" optimization. The solution is to apply an HTTP Host rule to disable that specific optimization for the problematic host. In this case, there was a defect that prevented such a rule from working on HTTP/2 connections.

- **STEELHEAD-20004** Symptom: The HTTP prepop feature does not work for HTTPS URLs.

Condition: The feature checks that the SSL blade is enabled, and the SSL blade was deprecated in 9.14.1. Subsequent releases no longer allow HTTPS URLs. The fix is to check the newer TLS enable status instead.

- **STEELHEAD-19932** Symptom: The optimization service crashes with error “SIGSEGV at ssltun::SSLTunHandlePool::put_ssl_handle.”
  Condition: The service can crash while shutting itself down after a service or system restart.

- **STEELHEAD-19690** Symptom: In some circumstances the system can generate WARN level messages of "Failure adding response executor - stream= 5089 - [RspAbort]."
  Condition: These messages were associated with non-error HTTP/2 reset frames and should not have been issued at WARN level. Actual errors will still generate a log entry but these have been filtered.

- **STEELHEAD-19338** Symptom: BIOS v0.46 is available in the RiOS image for the CXA580, CXA780, and CXA3080 appliances. The BIOS update disables certain power management features (ASPM) that can lead to unexpected issues with the on-board Ethernet interfaces. ASPM should be disabled in high-availability environments.
  Condition: To upgrade the BIOS, ensure the appliance is running a software version that contains the update, enter the *hardware rfut enable* command, and reboot the appliance. On the subsequent boot, the appliance will upgrade the BIOS and undergo a second reboot to apply the update.

- **STEELHEAD-19264** Symptom: Updates to support TLS 1.3 exposed a problem with SCEP requests over TLS if using HTTP/1.0. Support for HTTP/1.1 already exists and is the default.
  Condition: This issue does not have any adverse effects as HTTP/1.1 has been the standard version of HTTP since 1997.

- **STEELHEAD-18676** {{Details:}} OpenSSH version 7.4p1 on SteelHead is affected by CVE2019-6110, CVE-2020-14145, CVE-2018-20685, and CVE-2023-38408 vulnerability. {{Fix:}}

OpenSSH version on SteelHead is upgraded to version 9.4p1 with the fix to mitigate this vulnerability. {{Recommendation}}: Upgrade to a RiOS version with the fix.

- **STEELHEAD-18117** Symptom: A policy push with a high number of SSL whitelist domains fails with a timeout error.
  Condition: For whitelisted domains, more than 100 entries in a policy push fails in builds earlier than version 9.15.0. For builds earlier than version 9.15.0, a web proxy policy push fails with this error: !Screenshot 2023-11-06 at 11.46.09 AM (655e9fc5-45c5-41d5-93c58c58260a989e).png|width=1670,height=735!

- **STEELHEAD-18116** Symptom: When a SaaS Accelerator deployment is undeployed, the SaaS update was not free to do a complete cleanup of in-path rules. It cleaned up only what it could, so the page was not loading.
  Condition: As part of this fix, the In-path rules page should load when the parent application “office365” is deleted from mgmtdb nodes despite of the child application “msauth” being used in an in-path rule.

- **STEELHEAD-18102** Symptom: A duplicate Template ID is observed in cflow packets. Condition: Relates to Netflow.

- **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-17512** Symptom: The RiOS optimization service unexpectedly terminates. Condition: SMB2/3 secure optimization is not configured at the server-side SteelHead, and SMB3 traffic is blacklisted.

- **STEELHEAD-17444** Symptom: An smb_alert is raised when SteelHead has not joined the domain.
  Condition: This issue occurs when the SteelHead has not joined the domain but the WinSec Controller is configured or replication users are added in the SteelHead and the auth request times out due to not receiving a response within 60 seconds.

- **STEELHEAD-17418** Symptom: Citrix client versions later than 19.12.6 are not supported by Riverbed's latency optimization. Citrix traffic from unsupported client versions is passed through for latency optimization, but available for bandwidth optimization.
  Condition: The unsupported Citrix clients fail to connect to the server due to an issue in the pass-through logic of the latency optimization. With the bug fix, the traffic is correctly passed through without latency optimization and the unsupported Citrix client successfully connects to the Citrix server.

- **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-17290** Symptom: SMB2 memory leaks trigger the memory admission control alarm on SteelHead.
  Condition: This issue occurs due to excessive memory usage. SMB2 clients abruptly disconnect without closing files or logging off.

- **STEELHEAD-17289** Symptom: Outlook may not connect with eMAPI-OA NTLM delegation mode.
- Condition: Older versions of Outlook may not connect when Outlook Anywhere is configured to use delegation mode.

- **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-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-16982** Symptom: SMB2/3 optimization with Kerberos fails with the error "libnet_dssync failed. Unknown error."
  Condition: This issue occurs when the short domain name or NetBIOS name of the domain does not match the first portion of the Active Directory domain name.

- **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 inpath 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).

- **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-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-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-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, introduced in 9.14.1, is seen on all in-path LAN and WAN interfaces

- **STEELHEAD-16194** Symptom: SteelHead-v appliances on Hyper-V becomes inaccessible via CLI or web UI.

Condition: This issue can occur when a Hyper-V Steelhead appliance interface MTU is configured multiple times, and where that interface is the out-of-path optimization interface.

- **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-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-cx-specsheet.pdf|https://www.riverbed.com/sites/default/files/file/2023-02/steelhead-cx-specsheet.pdf]

- **STEELHEAD-15605** Symptom: On SteelHead, the *web-proxy ssl-domain <domain> includesan* 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-15052** Symptom: The domain rejoin operation shows successful even though the machine account is not created in the AD for the SteelHead, and the SteelHead is not able to perform protocol optimizations.
  Condition: This issue occurs when attempting the domain rejoin from the SteelHead after changing the domain controller name and the rejoin button is pressed.

- **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/site-packages/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-14573** Details: The current BIND version, 9.9.9_P5, is affected by CVE-202125215. The way DNAME records are processed may trigger the same RRset to the ANSWER section to be added more than once, which causes an assertion check to fail. The highest threat from this flaw is to system availability. Recommendation: Upgrade to a version that contains this bug fix. Fix: Patched the BIND package with the fix for CVE-2021-25215.

- **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-13362** Symptom: An endless disconnect/reconnect loop occurs in connection forwarding.
  Condition: Adding a new NetFlow collector can cause issues in SteelHead and Interceptor clusters.

- **STEELHEAD-13351** Symptom: When refreshing the Current Connections Page a system fault may be seen.
  Condition: This issue can occur on large data center appliances where the number of active connections is in upwards of several thousand.

- **STEELHEAD-13019** Symptom: The file copy operation on an SMB2 session fails with an error. The SteelHead logs the message "unexpected state=ERROR_SMBSIGNX_ACCESS_DENIED" on the affected connection.
  Condition: The SMB2 client uses anonymous logon to connect to a server.

- **STEELHEAD-12098** Symptom: Too few peers are listed for the *show peers online-only* CLI command.
  Condition: For the extended peer table (EPT), if many peers are offline, fewer online peers will be listed.

- **STEELHEAD-10919** Symptom: The system becomes inaccessible via SSH and Web GUI and requires a hard reset.
  Condition: This issue is specific to the CXA3080. Note: The fix for this issue is in firmware added to the RIOS image. Contact support for instructions on checking and applying that firmware (which is done outside of a regular RIOS upgrade).

- **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.

2) KNOWN ISSUES

- **STEELHEAD-19356** Symptom: Repeated syslog errors such as: {noformat}Sep 25 15:39:25 oak-sh1403 pm[10926]: [pm.ERR]: Output from yarder_rbt: StalePointInsertionError:

/var/opt/tms/ljstats/sh.appstats.optimized.app/0.rrd: illegal attempt to update using time 1695674365 when last update time is 1695691390 (minimum one second step) Sep 25 15:39:25 oak-sh1403 lumberjack_rbt[16386]: [sh.appstats.collector.ERROR] Exception '/var/opt/tms/ljstats/sh.appstats.optimized.app/0.rrd: illegal attempt to update using time 1695674365 when last update time is 1695691390 (minimum one second step)' in collecting stats {noformat}
Condition: This can occur when changing timezone configuration. There is no functional impact to the system, but to stop the errors from filling the logs, please contact support to workaround this problem.

- **STEELHEAD-19349** Steelhead cannot connect to a remote keystone server over an ipv6 network

- **STEELHEAD-19177** Symptom: Web-Proxy service status is in a degraded state Condition: This can occur after the system has been rebooted.

- **STEELHEAD-17163** Symptom: A notification of a SteelHead process failure occurs on domaind.
  Condition: This issue can occur after a system restart, but there is no functional impact to the system as domaind will start successfully.

- **STEELHEAD-16902** Symptom: If the “Enable Password Replication Policy” (PRP) is enabled for the Kerberos replication user: * The SMB optimization with Kerberos Authentication fails with the error “KDC has no support for encryption type” and the connections get blacklisted. * “Test Replication PRP” test fails with the error “KDC has no support for encryption type.”
  Condition: This issue occurs when the RC4 encryption type support is disabled in the domain controller(s).

- **STEELHEAD-16596** Symptom: Auto-negotiation is still active even if speed and/or duplex are hard-coded in the configuration. A link may be established in half-duplex when the connected switch interface has been hard-coded to 100/Full.
  Condition: This issue can occur on on-board 1G interfaces on the CXA580, CXA780, and CXA3080 models, in RiOS 9.14.1 and later.

- **STEELHEAD-13896** Symptom: After increasing the VCX model spec, the "connection pooling" value gets reset back to 20, breaking Steelhead-Steelconnect-EX compatibility mode. A value of "0" is required.

- **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.

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

3) 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*.

4) 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.

5) 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.

riverbed

6) HARDWARE AND SOFTWARE REQUIREMENTS

Steelhead appliance models supported for upgrade to this release:

- CXA580, CXA780, CXA3080, CXA5080, CXA7080
- VCX10, VCX20, VCX30, VCX40, VCX50, VCX60, VCX70, VCX80, VCX90, VCX100, VCX110
- AWS and Azure Cloud

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.*

7) 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.

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.