RIVERBED STEELHEAD CX v8
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

Version 1, Release 2

25 October 2019

Developed by Riverbed Technologies and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Riverbed SteelHead CX v8 Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the Riverbed SteelHead CX Wide Area Network (WAN) optimization solution. The STIG is a package of two STIGs that together ensure both the network backplane and the WAN optimization functions are secured.

The Riverbed SteelHead CX WAN optimization solution consists of the Riverbed Optimization System (RiOS) software and the Steelhead hardware or virtual appliance. The primary difference between the hardware appliances in the series is the number of WAN ports available and bandwidth capabilities. The RiOS software can also be hosted on a customer-provided host and implemented using a virtual appliance.

In order to perform its traffic and application functions, RiOS helps increase the security posture of the organization by performing deep packet inspection and analysis. This provides a security benefit to the organization because this gives visibility on network traffic by reporting on application usage. This data can be sent to enterprise performance management tools capturing key performance metrics for further analytics by tools.

While the Riverbed SteelHead CX v8 Network Device Management (NDM) STIG can be used to secure the management functions of all Steelhead products that use RiOS v8.x.x, the scope of the Riverbed SteelHead CX v8 Application Layer Gateway (ALG) STIG includes only SteelHead CX implementations.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

The STIG is a package of two STIGs that together ensure both the network backplane and the WAN optimization functions are secured. The Riverbed SteelHead CX v8 NDM STIG contains requirements that address the management and backplane functions of the RiOS. RiOS is installed on all of the Riverbed SteelHead products. While the Riverbed SteelHead CX v8 NDM STIG can be used to secure the management functions of all Steelhead products that use RiOS v8.x.x, the Riverbed SteelHead CX v8 ALG STIG should be used only for SteelHead CX assessments.

For assessments using the SteelHead CX virtual appliance, an assessment of the host using the applicable operating system STIG (e.g., Windows or Linux) must be performed. Also, an assessment of applications cohosted on the host is also required.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Overview

WAN optimization is an important part of the enterprise network strategy. With the increasing move to enterprise and cloud services, applications are being migrated to data centers or the Cloud, which moves them farther away from users. The need for access by remote and mobile users also drives the increasing need to prevent the WAN from being a performance bottleneck.

The SteelHead CX provides WAN optimization at OSI Layers 1, 4, and 7 to perform three major functions: perform data, transport, and application streamlining. RiOS combines fine grain data reduction and compression to perform data streamlining, reducing bandwidth. Transport and application streamlining minimize protocol and application communication redundancy by reducing packet round trips.

The SteelHead CX WAN optimization solution can also be configured to provide path optimization and Quality of Service (QoS). An organization can optimize some or the entire available network communications path, depending on the architecture implemented. Organizations can assign each optimized application a QoS class and can granularly assign each application class to a path. This configuration can be leveraged to create primary and secondary paths to each application based on the priority or other characteristics of the traffic. This path selection system would also ensure bandwidth failover of the primary communications pathway.

3.2 Architecture

Optimally, the SteelHead must be architecturally placed at the perimeter in front of the perimeter router and inline. Thus, traffic must be directed for firewall and Intrusion Detection and Protection System (IDPS) inspection for inbound and outbound traffic in compliance with DoD policy. Additionally, from an operational perspective, this architecture avoids the need to open many ports and services in the firewall to accommodate TCP options 76 and 78 and ports 7800, 7810, and 7870. Some other configurations may involve even more ports and services.

When the solution is implemented using a Steelhead CX hardware appliance implementation consisting of the RiOS installed on the SteelHead, administrators are not able to install any software that is not part of a Riverbed upgrade. RiOS enforces this by performing a validity check when an upgrade is attempted.

However, the RiOS application suite is available in a virtual appliance version which can be installed on an organization-provided host. This type of implementation adds risk because more ports may need to be opened in the firewall if placed in the recommended logical position in the architecture after the router and before the firewall and IDPS. The traffic should then be routed for inspection after traversing the WAN optimizer.