HPE 3PAR STORESERV OS
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

24 July 2024

Developed by HPE and DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

1. INTRODUCTION

1.1 Executive Summary

The HPE 3PAR StoreServ OS Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This document is meant for use in conjunction with other STIGs, such as the Enclave, Network Infrastructure, Secure Remote Computing, and appropriate application STIGs. The HPE 3PAR StoreServ OS STIG comprises the following individual STIGs:

- HPE 3PAR StoreServ 3.3x STIG.
- HPE 3PAR SSMC Operating System STIG.
- HPE 3PAR SSMC Web Sever STIG.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that 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 [National Security Agency/Central Security Service], 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 provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must 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

Category	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 DOD 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 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.

1.6 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 AO. 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 DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.7 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). Department of Defense 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 in accordance with (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) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. SECURITY ASSESSMENT INFORMATION

2.1 StoreServ User Accounts

The following vendor-recommended user account names are specified as literal values in several STIG check and fix instructions. These account names may be changed if desired. If changed, the appropriate check and fix actions must be modified accordingly:

- 3paradm.
- 3parsnmpuser.

The user account "3parsvc" is used for programmatic operations from the service processor. This account cannot be renamed and must not be removed. This is not an interactive user account, and the password is a random value for service processor use only.

Use of the service processor is restricted to actions related to firmware updates. When the service processor is in use, the following accounts are established on the host and the account names cannot be changed:

- 3parbrowse.
- 3paredit.
- 3parservice.

2.2 Port Scanner

The STIG references the use of "nmap" on a remote host to scan the open ports on the HPE 3PAR system. This action is not a required step to determine the state of the host's firewall settings. Other port scanning tools can be substituted. However, if a port scan shows any ports beyond those permitted in the STIG, it must be considered a finding.

2.3 Service Processor

Firmware updates are accomplished via the service processor. The service processor must remain off except during firmware updates. The use of service processor is limited only to times of updates to the system firmware.

It is recommended that the vendor's support organization perform updates for 3PAR systems that are STIG compliant. Following the firmware update and the disabling of the service processor, it is important to use the "removespcredential" command to remove temporary accounts associated with the service processor.

2.4 SSMC User Accounts

The following vendor-controlled user account names are specified as literal values in several STIG check and fix instructions:

- ssmcadmin.
- ssmcaudit.

The ssmcadmin is a privileged administrative group user account with just enough privileges to administer SSMC web server and/or appliance and application only. The ssmcaudit is a nonprivileged group user account that can introspect into the appliance filesystem for vulnerability scans (read-only filesystem bind-mounted within a jail-root).

There are no other nonprivileged users that can administrate SSMC by escalating their privileges.