VMWARE VSPHERE 6.7
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

27 October 2022

Developed by VMware 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

Page

1. INTRODUCTION

1.1 Executive Summary

The VMware vSphere 6.7 Security Technical Implementation Guides (STIGs) provide security policy and configuration requirements for the use of vSphere 6.7 in the Department of Defense (DOD). The VMware vSphere 6.7 STIG comprises the following individual STIGs:

- VMware vSphere 6.7 vCenter STIG.
- VMware vSphere 6.7 Virtual Machine STIG.
- VMware vSphere 6.7 ESXi STIG.
- VMware vSphere 6.7 EAM Tomcat STIG.
- VMware vSphere 6.7 Perfcharts Tomcat STIG.
- VMware vSphere 6.7 STS Tomcat STIG.
- VMware vSphere 6.7 UI Tomcat STIG.
- VMware vSphere 6.7 Photon OS STIG.
- VMware vSphere 6.7 PostgreSQL STIG.
- VMware vSphere 6.7 RhttpProxy STIG.
- VMware vSphere 6.7 VAMI-lightttpd STIG.
- VMware vSphere 6.7 Virgo-Client STIG.

The VMware vSphere 6.7 STIGs presume operation in an environment compliant with all applicable DOD guidance.

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

	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 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 Controlled Unclassified Information (CUI) will be available for 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 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.

1.8 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). 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. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

VMware vSphere 6.7 includes a number of components, each requiring separate STIG coverage. The following STIGs have been developed for vSphere 6.7 components. As STIGs are developed for other vSphere 6.7 components, they will be included here.

2.1.1 VMware vSphere 6.7 ESXi STIG

The VMware vSphere 6.7 ESXi STIG must be used to enhance the security configuration of the ESXi hypervisor hosting virtual machines.

2.1.2 VMware vSphere 6.7 Virtual Machine STIG

The VMware vSphere 6.7 Virtual Machine STIG must be used to enhance the security configuration of virtual machines hosted by the ESXi 6.7 hypervisor.

2.1.3 VMware vSphere 6.7 vCenter STIG

The VMware vSphere 6.7 vCenter STIG must be used to enhance the security configuration of the vCenter Server management application running on the Windows operating system. Its use is not mandatory for sites using a single ESXi hypervisor.

2.1.4 ESX Agent Manager (EAM)

The EAM automates the process of deploying and managing vSphere ESX Agents while extending the function of an ESXi host to provide additional services that a vSphere solution requires. EAM deploys agent VMs, installs VIBs in ESX, and integrates with DvFilter.

2.1.5 Security Token Service (STS)

The STS issues, validates, and renews security tokens for vCenter. STS authenticates the vCenter users based on the primary credentials and constructs a SAML token that contains user attributes.

2.1.6 VMware Appliance Management User Interface (VAMI UI)

The VAMI is a distinct interface that manages appliance-level functions such as host name, basic networking, NTP, updates, syslog, root password reset, and more.

2.1.7 Performance Charts (perfcharts)

Perfcharts collects and processes statistical performance data for managed entities into reports in image format, which it provides to the vSphere Web Client.

2.1.8 vSphere Client

vSphere Client is the Older, Flash-based vCenter user interface.

2.1.9 vSphere UI

vSphere UI is the new, HTML5 vCenter user interface.

2.1.10 rhttpproxy

The rhttpproxy is a simple, light service that aggregates and reverse proxies vCenter services. This simplifies ports and certificate management by having one point of entry from a vCenter component perspective.

2.1.11 Photon OS

Photon OS is VMware’s own Linux distribution. It is maintained internally and designed for VMware’s purposes, with nothing extra that VMware does not need.

2.1.12 PostgreSQL

PostgreSQL is the database.