

UNCLASSIFIED



# **VMWARE VSPHERE 6.0 ESXi SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW**

**Version 1, Release 4**

**28 July 2017**

**Developed by VMware and DISA for the DoD**

UNCLASSIFIED

## **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 DISA of any non-Federal entity, event, product, service, or enterprise.

**TABLE OF CONTENTS**

|  | <b>Page</b> |
|--|-------------|
| <b>1. INTRODUCTION.....</b>                                    | <b>1</b>    |
| 1.1 Executive Summary .....                                    | 1           |
| 1.2 Authority .....  | 1           |
| 1.3 Vulnerability Severity Category Code Definitions .....     | 1           |
| 1.4 STIG Distribution.....                                     | 2           |
| 1.5 SRG Compliance Reporting.....                              | 2           |
| 1.6 Document Revisions .....                                   | 2           |
| 1.7 Other Considerations.....                                  | 2           |
| 1.8 Product Approval Disclaimer.....                           | 3           |
| <b>2. ASSESSMENT CONSIDERATIONS.....</b>                       | <b>4</b>    |
| 2.1 Security Assessment Information .....                      | 4           |
| 2.1.1 VMware vSphere 6.0 Virtual Machine STIG.....             | 4           |
| 2.1.2 VMware vSphere 6.0 vCenter Server for Windows STIG ..... | 4           |

## LIST OF TABLES

|   | <b>Page</b> |
|---|-------------|
| Table 1-1: Vulnerability Severity Category Code Definitions ..... | 1           |

## 1. INTRODUCTION

### 1.1 Executive Summary

The VMware vSphere 6.0 ESXi (ESXi 6.0) Security Technical Implementation Guide (STIG) provides security policy and configuration requirements for the use of the ESXi 6.0 hypervisor in the Department of Defense (DoD).

The ESXi 6.0 STIG presumes operation in an environment compliant with all applicable DoD guidance.

### 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 provides 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 <b>directly and immediately</b> result in loss of Confidentiality, Availability, or Integrity. |
| CAT II  | Any vulnerability, the exploitation of which <b>has a potential</b> to result in loss of Confidentiality, Availability, or Integrity.            |
| CAT III | Any vulnerability, the existence of which <b>degrades measures</b> 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 Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is <http://iase.disa.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](mailto: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](mailto: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](mailto: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 #1
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<http://csrc.nist.gov/groups/STM/cmvp/>) IAW Federal/DoD mandated standard
- DoD Unified Capabilities (UC) Approved Products List (APL) (<http://www.disa.mil/network-services/ucco>) IAW DoDI 8100.0

## **2. ASSESSMENT CONSIDERATIONS**

### **2.1 Security Assessment Information**

The ESXi 6.0 STIG is to be used in conjunction with other VMware vSphere 6.0 STIGs.

#### **2.1.1 VMware vSphere 6.0 Virtual Machine STIG**

The VMware vSphere 6.0 Virtual Machine STIG must be used to enhance the security configuration of virtual machines hosted by the ESXi 6.0 hypervisor.

#### **2.1.2 VMware vSphere 6.0 vCenter Server for Windows STIG**

The VMware vSphere 6.0 vCenter Server for Windows STIG must be used to enhance the security configuration of vCenter Server management application running on the Windows operating system. Its use is not mandatory for sites using a single ESXi hypervisor.