RED HAT ENTERPRISE LINUX 6
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 14

27 January 2017

Developed by Red Hat, NSA, and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Red Hat Enterprise Linux 6 (RHEL6) Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements were developed from Federal and DoD consensus, based upon the Operating System Security Requirements Guide (OS SRG).

SRGs are collections of requirements applicable to a given technology area. SRGs represent an intermediate step between Control Correlation Identifiers (CCIs) and STIGs. CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in policy, such as those originating in Department of Defense (DoD) Instruction (DoDI) 8500.2 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for the product's technology area. The OS SRG contains general requirements for operating systems; this SRG may be used as a guide for enhancing the security configuration of any operating system.

The vulnerabilities discussed in this document are applicable to RHEL6 Desktop and Server editions. This document is meant for use in conjunction with the Enclave, Network Infrastructure, Secure Remote Computing, and appropriate application STIGs.

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 **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 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.

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 Command Examples

Some check and fix procedures contain example commands that can be used to obtain information regarding compliance with a requirement or to change a setting to attain compliance with a requirement. These example commands assume use of a standard UNIX shell operating as the root user. If the software used by these commands is not present on the system, the System Administrator (SA) or the reviewer is responsible for determining compliance with the requirement using the tools available on the system. Check procedures also contain instructions for evaluating compliance based on the output of these commands.

2.2 Alternate Software

RHEL6 systems offer extreme flexibility in replacing components provided by Red Hat with other software to meet operational needs. Many of the check and fix procedures in the RHEL6 STIG assume the use of the software provided by Red Hat. If alternate software is used to provide a function ordinarily provided by a default system application, the specific check and fix information for that function is no longer valid. The SA or the reviewer is responsible for evaluating the requirements based on documentation available for the alternate software. The system accreditation package must contain information pertaining to the use of alternate software.

2.3 Requirements for Disabled Functions

The RHEL6 STIG defines requirements for the further hardening and configuration of system functions that are required to be disabled. These requirements exist to address vulnerabilities in the system resulting from accidental activation, malicious intentional activation, or intentional activation of the system function based on acceptance of risk by the Authorizing Official (AO). Requirements for a system function remain applicable even when the system function is disabled. Requirements pertaining to software that is not installed on the system, and which has no remaining configuration files on the system, may be evaluated as NA.

3. SOFTWARE PATCHING GUIDELINES

Maintaining the security of an RHEL6 system requires frequent reviews of security bulletins. Many security bulletins and Information Assurance Vulnerability Management (IAVM) notifications mandate the installation of software patches to overcome noted security vulnerabilities. The SA will be responsible for installing all such patches. The Information System Security Officer (ISSO) will ensure the vulnerabilities have been remedied. DISA guidelines for remediation, including IAVMs, are as follows:

- Apply the applicable patch, upgrade to required software release, or remove the binary/application to remediate the finding.
- Or, the mode of the vulnerable binary may be changed to 0000 to downgrade the finding (for example, a CAT I finding may be downgraded to a CAT II).

SAs and ISSOs will regularly check Red Hat's vendor and third-party application vendor websites for information on new vendor-recommended updates and security patches that are applicable to their site. All applicable vendor-recommended updates and security patches will be applied to the system. A patch is deemed applicable if the product is installed, even if it is not used or is disabled.

4. OPEN SOURCE SOFTWARE (OSS) POLICY

On 16 October 2009, DoD CIO provided clarifying guidance regarding Open Source Software (OSS), reminding the DoD to take advantage of the capabilities available in the Open Source community as long as certain prerequisites are met. The 2009 memo can be found online at:

http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf

It reads:

> "Software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software. In other words, OSS is software for which the source is "open.""

Note: Red Hat Enterprise Linux 6, while meeting the DoD CIO definition of Open Source Software, is still considered Commercial-Off-The-Shelf (COTS) and requires purchase from the vendor.

Additionally, per Section 2(d) of the 16 Oct 2009 DoD CIO memo:

> "…the use of *any* software without appropriate maintenance and support presents an information assurance risk. Before approving the use of software (including OSS), system/program managers, and ultimately Authorizing Officials (AOs), must ensure that the plan for software support (e.g. commercial or Government program office support) is adequate for mission need."

The DoD CIO Open Source Frequently Asked Questions page can be found online, which provides educational resources for government employees and contractors to understand the policies and legal issues:

http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx