SUSE LINUX ENTERPRISE SERVER (SLES) V11 FOR SYSTEM Z SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 11

27 October 2017

Developed by 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 DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The SUSE Linux Enterprise Server (SLES) version 11 for System z Security Technical Implementation Guide (STIG) provides guidance for secure configuration and usage of Novell's SLES distribution. The STIG provides security guidance for deployments of SLES 11.x (where ".x" represents a service pack maintenance level) for IBM System z in a virtual operating environment (OE) managed by the z/VM hypervisor. This overview document gives technology-specific background and information on conducting a security review of SLES 11.x for only that platform.

SLES 11 for IBM System z requires 64-bit hardware (z9 or newer) and z/VM (version 5.4 or later). Other System z specific information pertaining to SLES 11 can be found in the Release Notes available on Novell's website: http://www.novell.com/linux/releasenotes/x86_64/SUSE-SLES/11-SP1/#s390x

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 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 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.

1.7 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). 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. TECHNOLOGY OVERVIEW

This section provides background information on SUSE Linux Enterprise Server (SLES) version 11 for System z and discusses general security considerations involved with using this technology as a virtual Operating Environment (OE) on IBM System z hardware.

This overview document is not intended as a comprehensive source of information on SLES. Since SLES is a UNIX-like OS, familiarity with the UNIX SRG and IBM z/VM Operating System are prerequisites to understanding how to implement these SLES STIG requirements on a System z server.

2.1 Introduction

SLES is a software distribution available from Novell/Attachmate. It is a server-oriented operating system based on the open-source Linux kernel. Many GNU tools and utilities are also included. The distribution is available for installation on five different platforms (x86, x86_64, Itanium, IBM Power, and IBM System z). This STIG is intended to provide guidance for SLES virtual operating environments running as z/VM guests on IBM System z hardware.

Linux is designed to be a modular and scalable operating environment. Organizations may choose from several topologies and install only the services and application needed to support their missions. Organizations may also extend the SLES environment through additional integration of locally developed or third-party products. SLES installations can host a variety of services, including but not limited to websites, portals, databases, and file servers.

2.2 Topology

SLES installations are supported on both standard Central Processor (CP) and Integrated Facility for Linux (IFL) engines. There is no difference from a security perspective. However, IFL engines are preferred for licensing and costing reasons.

The peripheral devices available to a Linux virtual OE running on System z are quite different from the options on a desktop/laptop or mid-tier system. The concept of a “console” to be used for offline system administration does not exist. The system “console” is accessed through a TN-3270-based z/VM user logon session. Console sessions must be encrypted and require a z/VM user ID and password. TN3270-based console sessions are not very useful for activities normally associated with a UNIX system console because there is no support for Xwindows (graphical) or ncurses (text-based) programs. Only line commands and line output are supported. Other devices that are not part of the System z build include audio, video, CD/DVD, floppy disk, and telephony (e.g., modem).

SLES can be deployed in a stand-alone LPAR without z/VM. However, the advantages of using z/VM make virtual OE implementations a much more attractive option. One advantage with System z and z/VM technology such as HiperSockets, Guest LAN, and VSWITCH, is the ability to configure a “network in a box”. Communication between virtual Linux OEs and other system(s) including z/OS can occur without a packet ever going “across the wire”, as long as all

guests and/or LPARs reside on the same System z server. This keeps real network traffic to a minimum while providing for the physical separation of web, application, and database environments. Recovery exercises are also simplified when such a configuration is used.

2.3 Product Dependencies

Hardware:

- z9 or newer processor
- Network connectivity (i.e., OSA, HiperSockets, VSwitch)

Software:

- z/VM 5.4 or later

2.4 Security Considerations

The SLES distribution is an integrated collection of system software and user space tools, utilities, and applications. Security considerations may be categorized into the following general areas:

- System Equipment
- Operating System
- File Integrity
- Development Systems
- Bootloaders and the Boot Process
- Kernel Configuration
- Pluggable Authentication Modules(PAM)
- Discretionary Access Control and General Security
- User Account Controls
- Logon Warning
- Account Access
- Inactivity Timeout/Locking
- Password Guidelines
- Root Account Controls
- File and Directory Controls
- Home directories and User files
- Run Control Scripts
- Global and Local Initialization files
- Shells
- Device files
- Set User ID (suid), Set Group ID (sgid), and Sticky Bit files

- Audit Requirements
- cron and at
- File Systems
- Syslog Facility
- Network Services
- inetd and xinetd
- rlogin, rsh, and exech
- finger
- Remote Printing
- traceroute
- sendmail or equivalent (i.e., postfix)
- FTP and Telnet
- X Window System
- Simple Network Management Protocol (SNMP)
- Secure Shell (OpenSSH)
- Routing
- NFS and Samba
- Security Tools
- Host Based Intrusion Detection
- Vulnerability Assessment
- Automatic Notifications
- Access Control Programs (tcpwrappers)

The SLES distribution includes a system administration tool called YaST2. This tool has both ncurses and X Windows -based interfaces, which can be used to perform various system administration tasks. Internally, YaST2 stores parameters for various options in the /etc/sysconfig tree. It then runs the SuSEconfig utility to keep its settings consistent with the respective system configuration files. If the system configuration files are edited directly over a period of time, a subsequent execution of YaST2/SuSEconfig can cause unpredictable results. To avoid this situation, use YaST2 whenever possible. If manual configuration is unavoidable, run /sbin/SuSEconfig from the command line after making such changes.

The YaST2/SuSEconfig toolset includes a permissions module. This module reads /etc/permissions.* files as configured in YaST2 to check and set file permissions whenever it is invoked. The /etc/permissions.local file is available for settings that should be applied last. Use of this file will ensure that subsequent package updates will not permanently undo locally applied settings. A secondary benefit of using the permissions.local file is to keep track of all permission settings that were changed from the vendor defaults. These settings can be applied manually at any time by issuing the command:

/sbin/SuSEconfig --module permissions

3. SECURITY READINESS REVIEW (SRR)

3.1 SRR Overview

The SLES 11.x review targets conditions that undermine the integrity of security, contribute to inefficient security operations and administration, or may lead to interruption of production operations. The items reviewed are based on standards and practices published by Novell/ Attachmate (the vendor) and other security guidance found in publications such as Department of Defense Instruction (DoDI) 8500.2 and National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 security controls.

Defense Information Systems Agency (DISA) has assigned a level of urgency to each finding based on Chief Information Officer (CIO)-established criteria for Certification and Accreditation (C&A). All findings are based on regulations and guidelines. All findings require correction by the host organization.

3.2 SRR Review Method

To perform a successful SRR, this document provides the methods to assess vulnerabilities on SLES virtual servers. In the initial release, all procedures are manual.