

UNCLASSIFIED



SPLUNK ENTERPRISE 8.X FOR LINUX SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 2

27 April 2022

Developed by 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 the Defense Information Systems Agency (DISA) of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
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
2. ASSESSMENT CONSIDERATIONS.....	4
2.1 Security Assessment Information	4
3. CONCEPTS AND TERMINOLOGY CONVENTIONS.....	5

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2

1. INTRODUCTION

1.1 Executive Summary

This Splunk Enterprise 8.x for Linux Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for deploying a hardened, secure Splunk instance in the organization.

Splunk Enterprise is a Security Information and Event Management (SIEM) product that enables the organization to collect, search, analyze, and report on any application, machine, or device data, such as Syslog, operating system events, websites, etc. Analyzing application, machine, and device data is a valuable forensic tool for maintaining organization confidentiality, integrity, and availability.

A SIEM product such as Splunk Enterprise is an expansion of the Central Log Server, and as such is often the mitigation point for logging requirements for other STIGs deployed in an organization. Because of this designation, several of the STIG requirements in this package address auditing and reporting of those upstream systems.

The ability to provide robust incident reports and alert notifications of events makes a SIEM product such as Splunk Enterprise a valuable tool for organizational security.

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

The Splunk Enterprise 8.x for Linux Security Readiness Review (SRR) ensures the site has properly provisioned and implemented the application and it is being managed in a way that is secure, efficient, and effective. The STIG identifies vulnerabilities that undermine security in that they have the potential to affect the confidentiality, integrity, or availability of the application. The items reviewed are based on standards and practices published by the DoD, their contractors, and other security guidance entities, following guidance published in the DoDI 8500.2 and NIST Special Publication (SP) 800-53 security controls.

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.

NIST Special Publications in the 800 series are of general interest to the computer security community. This series reports on Information Technology Laboratory (ITL) research, guidelines, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. The NIST 800 series Special Publications can be referenced at: <http://csrc.nist.gov/publications/PubsSPs.html>.

NIST SP 800-53, which is publicly available, is titled “Security and Privacy Controls for Federal Information Systems and Organizations”. It provides information security standards and guidelines, including minimum requirements for federal information systems. However, such standards and guidelines will not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

NIST SP 800-18, which is publicly available, is titled “Guide for Developing Security Plans for Federal Information Systems”. It provides both guidelines and a template for security plan creation and can serve as a base for development.

To perform a successful SRR, this document and accompanying STIG data provide the methods to assess vulnerabilities on deployed Splunk Enterprise systems.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

A typical Splunk Enterprise deployment includes three core components. These components may be combined in a small deployment or distributed in a large-scale deployment and are scalable based on organizational needs. Any or all of these components may be used more than once if the needs of the organization demand it.

- Forwarder: A forwarder collects relevant data and forwards it to the Splunk engines. Data can be taken in by many methods, such as text log files, Syslog data, TCP monitoring, operating system logs, and scripting.
- Indexer: This is the main engine of Splunk Enterprise. The indexer stores and indexes the data and responds to requests to analyze that data. Data is broken down into searchable fields and stored to help facilitate speedy analytical requests.
- Search Head: This is the main front end to Splunk Enterprise. The search head provides searching, reporting, and management of the deployment.

In a distributed environment, a Deployment Server is used.

In addition to the core components of Splunk Enterprise, this STIG requires use of an organizational-level user management system such as Lightweight Directory Access Protocol (LDAP), Active Directory, or a Security Assertion Markup Language (SAML) deployment. This STIG assumes that an LDAP, Active Directory, or SAML implementation is in place and functioning correctly. Removing the need for the application to manage users provides a better-controlled environment, mitigating the risk of inappropriate access or orphaned accounts.

In a DoD environment, support for the use of the CAC, containing Personal Identity Verification (PIV) certificates for access to the application, is also required. Supplemental documentation is supplied with this STIG package to address methods of providing CAC access to Splunk Enterprise LDAP, AD, or SAML accounts. These documents were developed and provided by the vendor to support DoD clients. They provide working examples but may be tailored to fit the user's environment.

Another concept that requires explanation *before* deployment is FIPS 140-2 compliance. For Splunk Enterprise to support FIPS 140-2, it *must* be enabled during the installation process. If this step is missed, the application must be reinstalled or an upgrade applied. The steps necessary to perform this requirement are included in the STIG and are documented on the vendor website.