National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Splunk 4.1.7

Report Number: CCEVS-VR-VID10437-2011
Version 1.0
March 18, 2011

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Validation Team

National Security Agency

Michelle Brinkmeyer

Lead Validator

The Aerospace Corporation

Jandria Alexander

Senior Validator

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is Splunk 4.1.7. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in March 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3. The evaluation was for Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.1 (Basic Flaw Remediation). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

Splunk collects IT data logs from various configured machines, stores the logs on disk, and indexes the data it collects. Splunk features search functionality to query these logs at based on user requests. Multiple instances of the Splunk process can be utilized in synchronization to optimize the functionality, with different Splunk processes focusing on collecting and forwarding IT data, storing and indexing IT data, and searching IT data and providing a collaborative user interface.

The Splunk product, when configured as specified in the Installation Guides and User Guides, satisfies all of the security functional requirements stated in the TOE's Security Target.

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The Splunk 4.1.7 Security Target version 2.0, dated 1 February 2011 identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Splunk product by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Evaluation Details

Evaluated Product	Splunk 4.1.7
Sponsor & Developer	Splunk, San Francisco, CA
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	March 2011
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.

CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL2 Augmented ALC_FLR.1
Description	The TOE is the Splunk product, which is a security software product developed by Splunk, Inc. as a Security Management product.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Splunk product by any agency of the U.S. Government, and no warranty of the Security Management product is either expressed or implied.
PP	None
Evaluation Personnel	Seyithan Ayhan Christopher Gugel Kevin Micciche Derek Scheer John Schroeder Amit Sharma
Validation Body	NIAP CCEVS Jandria Alexander Michelle Brinkmeyer

2.1 Threats to Security

Table 2 summarizes the threats that the evaluated product addresses.

Table 2 – Threats

A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or performs operations for which no access rights have been granted, via user error, system error, or other actions.
An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
A malicious user or process may view audit records and/or IT data, cause the records or information to be lost or modified, or prevent future audit records and IT data from being recorded, thus masking a user's action.
A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
A malicious user may attempt to communicate with the TOE's interfaces in ways that exploit flaws, subvert the TOE, or defeat the operation of its security mechanisms.
Users whether they be malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.
Users of an IT product the TOE monitors may perform undesirable actions using the IT product in question, whether by performing malicious actions upon the product, by utilizing functions within the IT product that adversely affect the system it interacts with, or by altering the configuration to be insecure.
A malicious user or process could perform suspicious activities against the TOE or objects in the Operational Environment monitored by the TOE without a TOE user authorized by the

Operational Environment becoming aware of this behavior.

3 Identification

The product being evaluated is Splunk 4.1.7.

4 Security Policy

4.1 IT Data Indexing

The TOE is able to collect and index IT data from the following log sources: Windows event logs, UDP and TCP syslog, Active Directory, generic scripted inputs, local disk logs, file system changes, and Windows registry changes. Each IT data event has at least the date/time of the event, source, source type, and host name. Only authorized users are able to read the indexed IT data by performing searches on the TOE. Authorized users are able to use the search functionality to search indexed audit logs based upon the data collected during indexing. All IT data logs indexed are protected from deletion or modification. In the evaluated configuration, the TOE is configured to stop indexing and begin to overwrite the oldest IT data records when storage reaches the configured limit, which is synonymous with the storage being full. The TOE also sends an alarm in the form of a user interface banner. In addition, the most recent stored IT records are maintained if storage runs out.

4.2 Security Audit

The TOE collects audit logs on TOE startup and shutdown, user login, and any user action on the system, including editing users and configuration. A timestamp is provided, as well as the user who performed the action (if applicable), the action itself, and a success or failure determination. Only authorized users are able to read this audit information by performing searches. The audit data collected is added to the index and is read in the same manner as IT data. The search functionality in the TOE allows authorized users the ability to read audit data to sort and filter the audit data returned to them based upon date/time of the event, type of event, subject identity, and outcome of the event, along with any other search parameters entered. All audit data logs are protected from deletion or modification. The most recent stored audit records are maintained if storage runs out.

4.3 Identification and Authentication

The TOE provides user accounts that have the following attributes: username, password, and roles. All users must successfully identify and authenticate themselves utilizing their username and password combination before they can make any TSF-related actions. There are two authentication mechanisms utilized in the TOE: Splunk authentication and LDAP authentication. Authorized users are able to select the authentication method used within the configuration options of the TOE. Upon authentication, users are bound to their role and other user attributes within a session object. A user session is terminated if the user is deleted or if all roles have been removed for the user. In addition, sessions will be terminated due to inactivity.

4.4 Security Management

The security management of the TOE is controlled by user actions that are authorized by the TOE's RBAC policy. Every function within the system, along with the objects it affects, is controlled by specific capabilities, indexes, or ACLs (Access Control Lists) available to the user performing the action. The security attributes are edited and assigned using this same RBAC policy. The primary security attributes within the system are roles. The default roles in the system are the following: admin, power, user, and can_delete. Additional roles can be generated by authorized users. One or more roles must be assigned to a user before the user can perform any TSF-related action on the TOE.

4.5 Protection of the TSF

The TOE utilizes OpenSSL to prevent unauthorized disclosure of data and detect modification of TSF data sent to the LDAP store. Detected modifications of TSF data will result in the packet being dropped. Additionally, OpenSSL is utilized to protect data being transferred between TOE components. OpenSSL is also used to create a logically distinct trusted path between remote users and the TOE, and will protect the TSF data in transit from unauthorized modification or disclosure. Remote users initiate the trusted path to the TOE. The trusted path is required to be used for user authentication, management actions, and data transfer.

4.6 Cryptographic Support

The TOE utilizes OpenSSL packages to generate cryptographic keys utilizing the RSA algorithm with 1024-bit keys. The TOE will overwrite old keys whenever a new key is generated. All sensitive interfaces are protected utilizing these encryption standards, including the user interface connections, connections between TOE components in the deployment, and the optional LDAP server.

4.7 High Availability

The TOE also provides mechanisms for high availability. The TOE will maintain a secure state whenever an indexer fails. The TOE will also ensure that the indexing functionality of the product will still operate if a single indexer fails.

5 Assumptions

5.1 Connectivity Assumptions

Table 1 – Connectivity Assumptions

The security features offered by the Operational Environment protect the files used by the TOE.
The network which the TOE is monitoring is expected to be secure to protect the transfer of data from remote data sources and email messages sent to the SMTP Server.

5.2 Personnel Assumptions

Table 2– Personnel Assumptions

One or more authorized administrators are assigned to install, configure and manage the TOE and the security of the information it contains.
Users of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation
System Administrators exercise due diligence to update the TOE with the latest patches and patch the Operational (e.g., OS and database) so they are not susceptible to network attacks.

5.3 Physical Assumptions

Table 3 – Physical Assumptions

The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

6 Clarification of Scope

The TOE includes all the code that enforces the policies identified (see Section 4).

The evaluated configuration of the TOE includes the Splunk 4.1.7 product that is comprised of the following:

- Splunk Web
- Splunk CLI
- Splunkd

6.1 System Requirements

The following components are recommended to run the TOE on the listed platforms:

Windows 7 (64 bit)

Processor	2x quad-core Xeon or equivalent at 3 Ghz
Disk space	200 GB
RAM	8 GB

Windows XP (32 bit)

Processor	2x quad-core Xeon or equivalent at 3 Ghz
Disk space	200 GB
RAM	8 GB

Windows Server 2008 R2 (64 bit)

Processor	2x quad-core Xeon or equivalent at 3 Ghz
Disk space	200 GB
RAM	8 GB

Windows Server 2003 (64 bit)

Processor	2x quad-core Xeon or equivalent at 3 Ghz
Disk space	200 GB

RAM	8 GB

Solaris 10 (64 bit)

Processor	2x quad-core Xeon or equivalent at 3 Ghz
Disk space	200 GB
RAM	8 GB

Red Hat 5.3 (64 bit)

Processor	2x quad-core Xeon or equivalent at 3 Ghz
Disk space	200 GB
RAM	8 GB

7 Architectural Information

The TOE's boundary has been defined in Figure 1, while Figure 2 shows a potential deployment of Splunk.

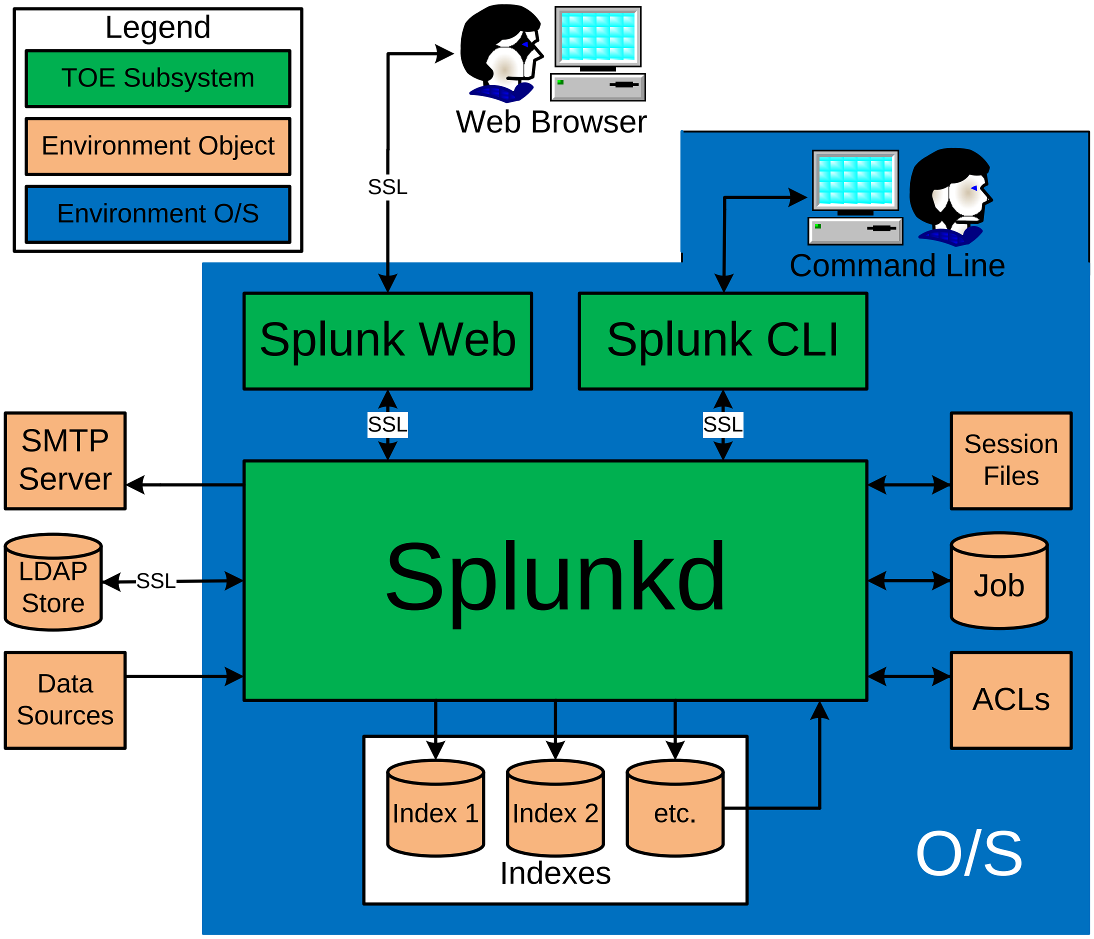

Figure 1 – TOE Boundary for Splunk 4.1.7

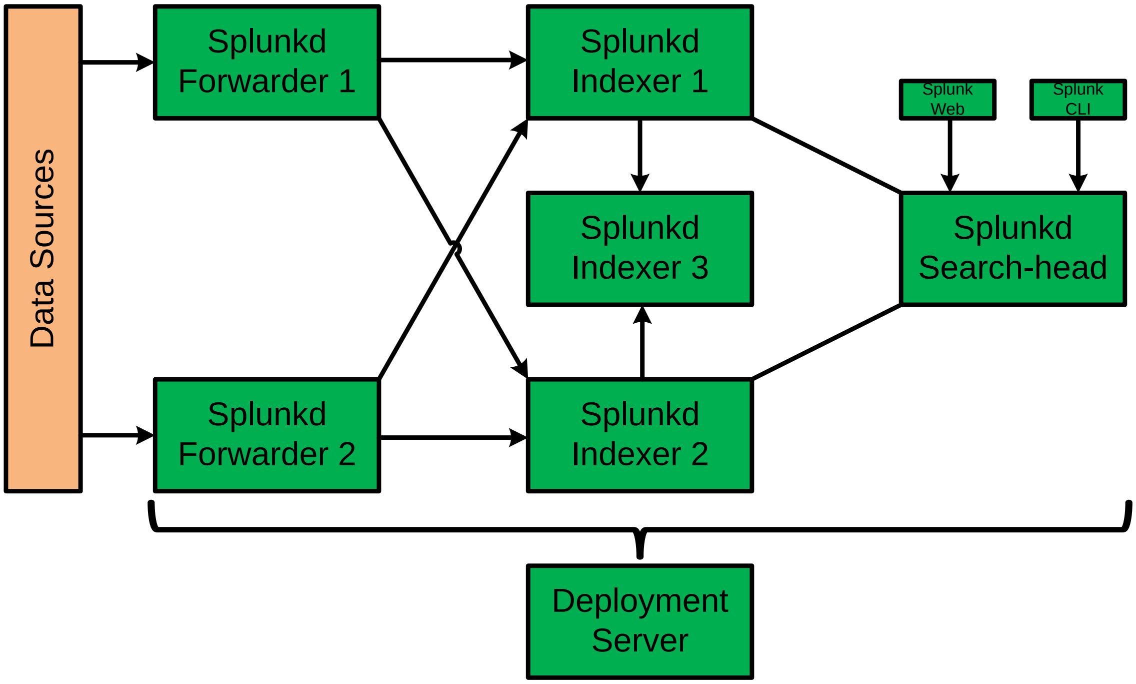

Figure 2 – TOE Deployment

7.1 TOE Components

7.1.1 Splunk Web

Python and browser-based interface that uses OpenSSL functionality and allows users to perform all management and searching functions on the TOE deployment. This subsystem is only utilized with the Splunkd process designated as the search-head.

7.1.2 Splunk CLI

Command-line interface that uses OpenSSL functionality and allows users to perform most management and searching functions on the TOE deployment. This subsystem is only utilized with the Splunkd process designated as the search-head.

7.1.3 Splunkd

Process that contains most of the Splunk primary functionality. This process contains modules to receive data, forward data, and index data. In addition, when searches are performed, this process performs the search on its configured indexes and returns the results to the search-head. In addition, scheduled searches can be configured by users. This process also contains a web server, handles all authentication and authorization needs, and can be configured to be a deployment server for configuration updates.

8 Documentation

These are public facing documents that were evaluated to satisfy assurance requirements:

Component	Document(s)	Rationale

Component	Document(s)	Rationale
AGD_OPE.1 Operational User Guidance	• Splunk Admin Manual Version: 4.1.7 • Splunk Application Management Version: 4.1.7 • Splunk Developer Manual Version: 4.1.7 • Splunk Installation Manual Version: 4.1.7 • Splunk Knowledge Manager Manual Version: 4.1.7 • Splunk Release Notes Version: 4.1.7 • Splunk Search Reference Version: 4.1.7 • Splunk User Manual Version: 4.1.7	These documents describe the operational user guidance for the TOE.
AGD_PRE.1 Preparative Procedures	• Splunk Admin Manual Version: 4.1.7 • Splunk Application Management Version: 4.1.7 • Splunk Developer Manual Version: 4.1.7 • Splunk Installation Manual Version: 4.1.7 • Splunk Knowledge Manager Manual Version: 4.1.7 • Splunk Release Notes Version: 4.1.7 • Splunk Search Reference Version: 4.1.7 • Splunk User Manual Version: 4.1.7	This document describes the preparative procedures that need to be done prior to installing the TOE.
ASE_CCL.1 Conformance Claims	Splunk 4.1.7 Security Target 2.0	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	Splunk 4.1.7 Security Target 2.0	This document provides a definition for all extended components in the TOE.

Component	Document(s)	Rationale
ASE_INT.1 Security Target Introduction	Splunk 4.1.7 Security Target 2.0	This document describes the Introduction of the Security Target.
ASE_OBJ.2 Security Objectives	Splunk 4.1.7 Security Target 2.0	This document describes all of the security objectives for the TOE.
ASE_REQ.2 Derived Security Requirements	Splunk 4.1.7 Security Target 2.0	This document describes all of the security requirements for the TOE.
ASE_SPD.1 Security Problem Definition	Splunk 4.1.7 Security Target 2.0	This document describes the security problem definition of the Security Target.
ASE_TSS.1 TOE Summary Specification	Splunk 4.1.7 Security Target 2.0	This document describes the TSS section of the Security Target.

Table 8 – Assurance Documents Evidence

9 TOE Acquisition

The NIAP-certified Splunk product is acquired via normal sales channels, and electronic delivery of the TOE is coordinated with the end customer by Splunk, Inc.

10 IT Product Testing

10.1 Functional Testing

10.1.1 Functional Test Methodology

The test team's test approach is to test the security mechanisms of the Splunk 4.1.7 by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface was described in the relevant design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), Security Architecture (ARC) and the vendor's test plans were used to demonstrate test coverage of all EAL2 requirements for all security relevant TOE external interfaces. TOE external interfaces that were determined to be security relevant are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements are associated with interfaces if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. *ri*

10.1.2 Functional Test Results

During the course of the evaluation, the Booz Allen evaluation team reviewed the vendor's functional testing and determined that all security relevant TOE external interfaces were tested and all of the claimed TSF functionality was tested by the vendor. The evaluation team then created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing developed by the evaluators. The evaluators test suite emphasized on the product's primary TSF functionality, and additional regression testing. The vendor and evaluator testing efforts performed both positive and negative testing of the Security Functional Requirements. The testing efforts ensured consistent results of TOE functionality performed on all Operating Systems included in the evaluation, and also verified that the TOE can perform in a heterogeneous environment where the TOE is installed across multiple Operating Systems in a TOE deployment (see Figure 2). Based upon the results of the vendor and evaluator testing; it has been determined that the product functionally operates as described.

10.2 Vulnerability Testing

10.2.1 Vulnerability Test Methodology

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.
- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Vulnerability Scanner (Nessus)
  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

Backdoors CGI abuses Denial of Service	Gain root remotely General Miscellaneous	RPC Settings SMTP Problems

Finger abuses
Firewalls
FTP
Gain a shell remotely
Netware
NIS
Port scanners
Remote file access
SNMP
Untested
Useless services

- Unauthenticated Access / Directory Traversal Attack
  This test used "URL hacking" to attempt to access protected TOE resources by injecting unexpected input into requests that were sent to the TOE. This was done using two different approaches to URL exploitation.
  - The first part attempted to access protected TOE resources as an unauthenticated outsider.
  - The second part attempted to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated).
- SQL Injection / Cross Site Scripting Attack / Cross Site Request Forgery
  This test executed automated SQL Injection and Cross Site Scripting attacks against the TOE. The evaluators determined any fields or variables that could be prone to attack. They then used a scanner, which contained a large database of standard strings that are used for testing SQL Injection and Cross Site Scripting issues. These strings were input into the various fields and variables and the output was analyzed for inconsistencies.
- Web Server Vulnerability Scanner (Nikto)
  This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interfaces. This scanner probed a wide range of vulnerabilities that included the following:

File Upload.
Interesting File / Seen in logs.
Misconfiguration / Default File.
Information Disclosure.
Injection (XSS/Script/HTML).
Remote File Retrieval
Denial of Service.
Command Execution / Remote Shell.
SQL Injection.
Authentication Bypass.
Software Identification
Remote source inclusion.

- Vulnerability Scanner (Retina)
  This test used the Retina Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.
  The scanner probed a wide range of vulnerabilities that included but was not limited to the following:

Accounts
Anti-Virus
Backdoors
CGI Scripts
Database Issues
DoS
IP Services
Registry
Remote Access
RPC Services
Service Control
Spyware
Web Services
CVE Issues
SecurityFocus BID Issues

- Data Source Injection Attack
  The TOE takes data from outside data sources and presents that data to TOE users in a web application. This test attempted to inject malicious data into the data source and ensure that the TOE properly escapes that data before presenting it

over the web interface. If a malicious user were able to inject Java Script into the data source and have it presented un-escaped to a browser, a cross site scripting attack could be possible.

- Syslog Spoofing
  In this test, the attacker attempted to spoof syslog messages from one of the data sources configured in the TOE.

10.2.2 Vulnerability Test Results

The following lists any issues that were discovered as a result of the vulnerability testing process. These issues have been broken up into the following categories:

10.2.2.1 Additional Guidance for Security

- **Default Web Server Uses HTTP**
  The default installation of Splunk automatically sets the web server to communicate through unencrypted HTTP. This is insecure as it would allow communication between the user and the Splunk Web to be sniffed by an untrusted party and leak information. The TOE only communicates via HTTP or HTTPS, but not both. The user guidance details how to configure the TOE to use HTTPS.

10.2.2.2 Informational Notes

- **Log Message Spoofing and Interception**
  Log messages are collected using syslog. The syslog protocol can be transmitted over TCP or UDP and is unencrypted on the network. This means that any syslog message could potentially be sniffed by an untrusted party and leak information prior to the syslog message being received by the TOE. In addition, syslog messages have no authentication of either the client or the server. Therefore messages can be forged that appear to come from a valid source and contain false information. The administrator should be aware of these facts and should not rely on the confidentiality or integrity of the collected IT data.

- **Use of Valid Certificates**
  All implementations of SSL in use by the product should be configured using valid certificates signed by a trusted certificate authority. The use of self-signed certificates could expose users to Man-In-the-Middle attacks resulting in credential theft.

11 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the Splunk 4.1.7 TOE meets the security requirements contained in the Security Target.

The criteria against which the Splunk TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the Splunk 4.1.7 TOE is EAL2 augmented with ALC_FLR.1. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in March 2011. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

12 Validator Comments/Recommendations

12.1 Cryptography is Vendor Asserted

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor. Users of the need to ensure that the data sources sent to the TOE are protected either as part of the environment or with SSL in the evaluated configuration. The Administrative guidance identifies those interfaces that use SSL and those that do not.

13 Security Target

The security target for this product's evaluation is Splunk 4.1.7 Security Target, Version 2.0, 1 February 2011.

14 List of Acronyms

Acronym	Definition
AD	Active Directory
ACL	Access Control List
CA	Certificate Authority
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CLI	Command-line Interface
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership

OS	Operating System
PP	Protection Profile
RAID	Redundant Array of Independent Disks
RBAC	Role Based Access Control
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
X.509	X.500 Series Standard for Public-key and Attribute and Certificate Frameworks

15 Terminology

Terminology	**Definition**
Access Control Lists	The owner of each created object specifies the read/write access available to each role within the system. Obviously, the owner of an object has unrestricted access to the objects it controls.
Authorized User	A user that has been assigned a role with the attributes that allow an action on an object as defined in Table 7-3. This essentially means “any user that is capable of performing the action in question.”
Capability	An action in the TOE that can be added to a role to grant the role the ability to perform said action.
Deployment Client	This refers to all Splunkd processes that are sent configuration updates by the Deployment Server.
Deployment Server	An instance of the Splunkd process that is configured solely to deploy configuration updates to the other Splunkd processes within the TOE deployment.
Forwarder	An instance of the Splunkd process that is configured solely to collect raw IT data logs, parse them, formulate indexed logs, and then forward both the raw data and the indexed logs to another configured Splunkd process.
Index	When used as a verb, this refers to the actual process of parsing raw data logs, extracting fields, and storing the parsed data. When used as a noun, this refers to where said parsed data is stored upon Splunkd processes configured as indexers.
Indexed Data	This refers to parsed IT data that is stored in an indexer.
Indexer	An instance of the Splunkd process that is configured to collect parsed data logs as well as raw data logs from a forwarder and to store said data.
IT Data	All data that the TOE collects and indexes.
Parsing	Specifically to Splunk, this is the act of utilizing Splunk’s indexing functionality to process raw data and extract specific default and user-defined fields. The output of this process is indexed data.
Raw Data	Unprocessed IT data the TOE collects from any configured source.
Receiver	Any Splunkd process that receives data from one or more forwarders.
Role	A named bundle of capabilities and allowed indexes that determines the amount of access specific users are allowed within the TOE. There are defaults, but additional roles can be user-generated. Roles are assigned to

	users.
Search-head	An instance of the Splunkd process that is configured solely to be the primary component for searching. It is also the only Splunkd process within the evaluated configuration to interface with users via the Splunk Web and Splunk CLI processes. This means that most of the general TOE management is utilized through this process exclusively.
Server Class	A deployment configuration shared by a group of deployment clients. A deployment client can belong to multiple server classes.
Splunk Object	A Splunk object is an object within the system that has an ACL defined for it.

16 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 3.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 3.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.
5. Splunk 4.1.7 Security Target, Version 2.0, February 1, 2011
6. Evaluation Technical Report for a Target of Evaluation “Splunk 4.1.7” Evaluation Technical Report v3.0 dated 7 February 2011.