National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Splunk Enterprise 6.4.5

Report Number: CCEVS-VR-VID107807-2017
Version 1.0
March 22, 2017

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

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell, Senior Validator
Sheldon Durrant
Dr. Patrick Mallett, Lead Validator
Lisa Mitchell
Linda Morrison
MITRE

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
Herbert Markle
Brad Isbell
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Annapolis Junction, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Splunk Enterprise 6.4.5 provided by Splunk. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton, Inc. Common Criteria Testing Laboratory (CCTL) in Annapolis Junction, Maryland, United States of America, and was completed in March 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR), Assurance Activity Report (AAR), and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements set forth in the Protection Profile for Application Software, version 1.2 (App PP).

The Target of Evaluation (TOE) is the Splunk Enterprise 6.4.5 software, which includes the Splunkd process and the Splunk Web and Splunk CLI administrative interfaces. The physical boundary for the TOE is the Splunk Enterprise 6.4.5 software installed on one or more host platforms running Red Hat Enterprise Linux 6.5, 64 bit.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the App PP document. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the Evaluation Team. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Splunk Enterprise 6.4.5 Security Target, Version 1.0*, dated January 20, 2017 and analysis performed by the Validation Team.

The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:

- TD0131: Update to FCS_TLSS_EXT.1.1 Test 4.5.

The Validators note that a required test for SFR FCS_TLSC_EXT.1.1 was waived as the result of a NIAP Technical Rapid Response Team decision that concluded that the test should have been classified at "Conditional" in the PP and was, therefore, due to the design of the TOE not required to be performed for this evaluation. A NIAP Technical Decision regarding that is expected to be released soon.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Splunk Enterprise 6.4.5
Protection Profile	Protection Profile for Application Software, version 1.2 (including all applicable NIAP Technical Decisions)
Security Target	Splunk Enterprise 6.4.5 Security Target, version 1.0, dated January 20, 2017
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Splunk Enterprise 6.4.5" Evaluation Technical Report v1.0 dated January 31, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Splunk
Developer	Splunk
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Annapolis Junction, Maryland
Validation Team	Paul Bicknell Sheldon Durrant Dr. Patrick Mallett Lisa Mitchell Linda Morrison The MITRE Corporation

3 Assumptions, Threats, and Clarification of Scope

3.1 Assumptions

The Security Problem Definition, including the Assumptions, may be found in the Protection Profile for Application Software, Version 1.2, 22 April 2016. That information has not been reproduced here and the App_PP should be consulted if there is interest in that material.

3.2 Threats

- The Security Problem Definition, including the Threats, may be found in the Protection Profile for Application Software, Version 1.2, 22 April 2016. That information has not been reproduced here and the App_PP should be consulted if there is interest in that material.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Application Software, version 1.2 (App PP), including all relevant NIAP Technical Decisions. A subset of the “optional” and “selection-based” security requirements defined in the App PP are claimed by the TOE and documented in the ST.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to security functionality not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. All other functionality provided by the software needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The TOE is a self-contained instance of Splunk Enterprise 6.4.5. In the evaluated configuration, there will be two or more instances of Splunk Enterprise 6.4.5 deployed and communicating with each other. One instance serves as an indexer that is responsible for aggregating non-TSF system generated data and one or more instances are configured as a forwarder that is responsible for collecting non-TSF system generated data on its underlying OS platform. The TOE includes all the code that enforces the functions identified (see Section 5).

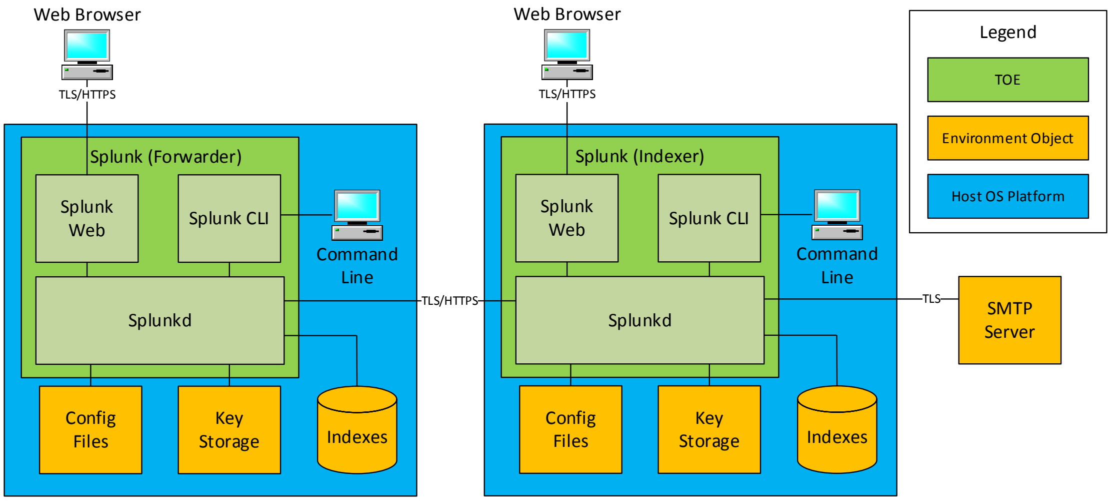
4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The TOE is Splunk Enterprise 6.4.5 ("Splunk"), which is an application on an operating system. The primary functionality of Splunk is to collect system generated IT data from various types of OS platform systems and aggregate it in a centralized location for real-time visibility and analysis of system behavior. Splunk can be deployed in a distributed manner so that multiple instances of the product can act as forwarders, each of which is responsible for sending its data to a centralized instance of the product that is responsible for indexing the data and providing search/reporting capability for it via administrative interfaces. The Target of Evaluation (TOE) is the Splunk application itself, the interfaces used to administer it, and the communications channel that is used to transmit data between forwarder system(s) and the indexer. The general application security functionality of Splunk is the product functionality that is being evaluated as part of the TOE.

Figure 1: Typical TOE Deployment



As illustrated in Figure 1, the TOE boundary contains 3 subsystems: Splunk Web, Splunk CLI, and Splunkd. Splunk Web and Splunk CLI are accessed through a supported web browser or command-line interface, respectively. Splunkd is the application process that provides most of the product functionality.

Splunk can act as either a forwarder (responsible for collecting system generated data from the general-purpose computer that it resides on) or an indexer (responsible for receiving system generated data from one or more other instances of Splunk). Regardless of how Splunk is configured to function, the underlying binary application is the same; there is no separate executable code. While the product vendor provides multiple versions of the product, only the full version of Splunk Enterprise 6.4.5 is considered to be the TOE – other product versions were not evaluated and no security claims are made for them.

When the Splunk application is administratively configured as a forwarder, the administrator may specify an indexer application to transmit the system generated data that it collects to a centralized location. This transmission is secured using TLS/HTTPS. When the Splunk application is administratively configured as an indexer, the TOE can connect with an SMTP server to send out configured alerts based on the indexer's analysis of the system generated data that it receives.

Splunk Web is a browser-based UI that supports Internet Explorer 11 and the latest versions of Google Chrome and Mozilla Firefox. It provides a graphical interface to the product in order to perform administrative activities or to view reports or other graphical displays of system data that is collected by Splunkd. Users authenticate to Splunk Web using username and password. The Splunk Web component is only responsible for receiving user inputs; all authorizations are performed by Splunkd.

Splunk CLI provides a command line interface to the product that can be accessed through a terminal application running on the host platform. It has the same functionality as the Splunk Web subsystem except for visual presentation functionality. A user uses this subsystem by navigating to the folder in which Splunkd resides. The user then issues the command "splunk" to run the executable along with any desired command-line arguments. For instance, a user would enter "splunk stop" to stop the Splunkd process.

Since Splunk is a standalone application that runs on a general-purpose computer (i.e. user's workstation), a single instance of the product is managed individually. If multiple instances of Splunk are configured as forwarders and transmit data to a Splunk instance configured as an indexer as defined by the evaluated configuration, this would be specified during initial setup of each Splunk instance as well as any further management. Thus, the multiple instances of Splunk in the evaluated configuration are not centrally managed as a distributed product.

Splunkd is the subsystem that consists of most of the functionality in the product. This subsystem handles identification, authentication, and authorization of users to access the application and interact with its administrative functions. The primary functionality of the product from a user perspective is to search accumulated IT data. A user issues a search command, which will search all of the indexes that the user has access to assuming they have the privilege to search. Every search entered by a user starts a new Splunkd process that only performs that search, and returns the result to the parent Splunkd process. This data is then returned to the user, and there are a set of actions that a user can perform with this search and the search data. Because the focus of the claimed Protection Profile is the general security of the application and how it interfaces with its underlying platform, only the functionality that is part of the claimed Protection Profile is considered to be part of the TOE. This functionality is described in more detail in section 5 below.

Instances of Splunk that are configured as forwarders are installed on the systems from which logs will be collected and sent to the indexer. The sole function and communication pathway of the forwarders in the single instance configuration is to do this log collection and transfer to the indexer.

4.2 Physical Boundaries

The TOE is Splunk Enterprise 6.4.5 ("Splunk"), which includes the Splunkd process and the Splunk Web and Splunk CLI administrative interfaces. The TOE is a self-contained instance of Splunk Enterprise 6.4.5. In the evaluated configuration, the TOE's deployment will include a distributed collection of Splunk instances deployed on two or more host platforms. One instance of Splunk is configured as an indexer, which allows it to act as a server for receiving information from other instances of Splunk. One or more instances of Splunk are configured as a forwarder, which act as a client when sending data to the indexer.

The TOE resides on a network and supports the following hardware, software, and firmware in its operational environment:

Table 3 – Operational Environment Components

Component	Usage/Purpose Description for TOE performance
Host Platform(s)	A general-purpose computer on which the TOE is installed. In the evaluated configuration, at least two host platforms are used. The minimum system requirements for the host platforms in the evaluated configuration are: • Red Hat Enterprise Linux 6.5, 64 bit • 2x six-core, 2 GHz CPU (Intel Xeon x64) • 12 GB RAM • RAID 0 or 1+0 • 5 GB of free disk space
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE remotely via a web browser. Note that the host platform can also be used to administer the TOE locally.
SMTP Server	An email server that can receive alerts from the TOE and distribute them to users in the Operational Environment via email.

5 Security Policy

5.1 Cryptographic Support

The TOE uses NIST-validated cryptographic algorithm implementations to support the establishment of trusted channels and paths to protect data in transit. In the evaluated configuration, the TOE will act as a server for TLS/HTTPS to facilitate trusted remote communications. As an application on an operating system, the TOE interfaces with the operating system's key storage to securely store key data related to secure communications. The TOE also relies on the underlying platform to generate entropy that is used as input data for the TOE's deterministic random bit generator (DRBG).

5.2 User Data Protection

In the evaluated configuration, the TOE will reside on an encrypted disk partition on the underlying platform to secure its data at rest. The TOE protects data stored on the underlying platform by minimizing its use of platform resources. Specifically, the TOE will only use the underlying platform's network connectivity for administrative activities, email alerts that are generated with user approval, and administratively-configured transmission of system generated data from a forwarder instance of Splunk to an indexer.

5.3 Identification and Authentication

In order to facilitate secure communications using HTTPS, the TOE provides a mechanism to validate X.509 certificates. The TOE uses a CRL to check certificate expiration status but will permit certificates to be used (with a warning) when the CRL is unavailable.

5.4 Security Management

The TOE provides a default credential that is used for initial authentication that must be reset prior to any other TSF-mediated action being authorized. The files and directories that comprise the TOE are protected against unauthorized access by only permitting write access to the user that performed the installation.

The TOE provides several security-relevant management functions. Specifically, the TOE has the ability to configure how information about the underlying platform is transmitted over the network. The TOE also provides administrators with the ability to configure the behavior of the TLS/HTTPS trusted channel. Any changes to the TOE's configuration will be logged.

5.5 Privacy

The TOE ensures the privacy of its administrators and users by not providing any ability to transmit personally identifiable information (PII) over the network.

5.6 Protection of the TSF

The TOE protects against exploitation by implementing address space layout randomization (ASLR) and only allocating memory for both writing and execution for just-in-time (JIT) compilation. The TOE is also compatible with SELinux and is compiled with stack-based buffer overflow protection. It also prevents the writing of user-modifiable files to directories that contain executable files.

The TOE uses standard platform APIs and includes only the third-party libraries it needs to perform its functionality. The TOE version can be checked either through its management interfaces or through the underlying platform’s package manager. Updates must be manually downloaded to the platform’s file system and installed using the platform’s package manager. In the evaluated configuration, the administrator will download and install a public key from the TOE’s developer that is installed into the package manager and used to verify the integrity of any updates to the TOE.

5.7 Trusted Path/Channels

The TOE protects all data in transit using HTTPS over TLS or standalone TLS. TLS/HTTPS protocol is used to secure remote administration using the web GUI. It can also be used to securely send alerts to a remote SMTP server in the Operational Environment. TLS is used to secure communications between separate instances of Splunk, where the forwarder instance(s) act as the client and the indexer acts as a server.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Splunk® Enterprise Securing Splunk Enterprise with Common Criteria 6.4.5
- Splunk® Enterprise Admin Manual 6.4.5
- Splunk® Enterprise Installation Manual 6.4.5
- Splunk® Enterprise Securing Splunk Enterprise 6.4.5

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, the TOE's deployment will include a distributed collection of Splunk instances deployed on two or more host platforms. One instance of Splunk is configured as an indexer, which allows it to act as a server for receiving information from other instances of Splunk. One or more instances of Splunk are configured as a forwarder, which act as a client when sending data to the indexer.

To use the product in the evaluated configuration, the product must be configured as specified in the *Splunk® Enterprise Securing Splunk Enterprise with Common Criteria 6.4.5* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary *Evaluation Technical Report for a Target of Evaluation "Splunk 6.4.5" Evaluation Technical Report v1.0*, dated January 31, 2017, as summarized in the publicly available *Assurance Activity Report for a Target of Evaluation "Splunk 6.4.5" Assurance Activity Report v1.0,* dated February 1, 2017.

8.1 Test Configuration

The evaluation team conducted testing at Splunk's San Francisco, CA facility as well as at Booz Allen's CCTL on isolated networks. The evaluation team configured the TOE according the *Splunk® Enterprise Securing Splunk Enterprise with Common Criteria 6.4.5* document for testing. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces.

The TOE was configured to communicate with the following environment components:

- Red Hat Enterprise Linux Server release 6.5 (Santiago)
- x86_64 architecture (tested on Intel(R) Xeon(R) CPU E3-1220 v3)
- Security-Enhanced Linux (SELinux) with policy version 24
- SMTP Server
- Management Workstation (Firefox and Chrome web browsers)
- Second instance of Splunk

The following test tools were installed on a separate workstation (management workstation)

- WireShark version 2.2.3
- Nmap version 6.47

*Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to perform all the Test Assurance Activities contained in the App PP as well as test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR Test Assurance Activities as defined by the App PP for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* were 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 were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

The TOE successfully satisfied all these tests.

8.4 Evaluation Team Vulnerability Testing

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 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:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.
- Web Application Vulnerability Scan
  The Open Web Application Security Project (OWASP) Top 10 represents a broad consensus on the most critical web application security flaws. The errors on this list occur frequently in web applications, are often easy to find, and easy to exploit and therefore fall under the CC vulnerability analysis scrutiny. This covers injections, XSS, Cross Site Request Forgeries, Insecure Direct Object References, unvalidated redirects and forwards, misconfiguration, data exposure and weak session management.
- Force SSHv1
  This attack determines if the client will accept both SSHv1 and SSHv2 connections when the TOE claims to only support SSHv2
- Virus/Malware Scan
  Perform a virus scan on software as required by the App PP assurance activity requirements.

The TOE successfully prevented any attempts of subverting its security.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Evaluation Activities specified in the App PP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Splunk Enterprise 6.4.5product that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the App PP in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the App PP related to the examination of the information contained in the TOE Summary Specification.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the App PP related to the examination of the information contained in the operational guidance documents.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and the extended assurance requirement ALC_TSU_EXT.1 defined in the App PP. The evaluation team found that the TOE was identified and a method of timely updates was described.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Evaluation Activities in the App PP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and validated that the vendor fixed all findings with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the App PP were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the App PP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Splunk® Enterprise Securing Splunk Enterprise with Common Criteria 6.4.5*.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Splunk Enterprise 6.4.5 Security Target, version 1.0*, dated January 20, 2017.

13 List of Acronyms

Acronyms / Abbreviations	Definition
AES	Advanced Encryption Standard
ASLR	Address Space Layout Randomization
CA	Certification Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CLI	Command Line Interface
CRL	Certificate Revocation List
CSP	Critical Security Parameter
DHE	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
HMAC	Hashed Message Authentication Code
HTTPS	Hypertext Transfer Protocol - Secure
JIT	Just-in-Time (compilation)
PCRE	Perl Compatible Regular Expressions
RA	Registration Authority
RSA	Rivest Shamir Adelman (encryption algorithm)
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

14 Terminology

Term	Definition
Administrator	An administrator is an individual who has permissions to modify the behavior of the TOE. This includes the individual that installs it on the underlying platform but can also include other individuals if administrator access is granted to them on Splunk Web or Splunk CLI.
Splunk CLI	Splunk CLI is an application that can be used to interface with the TOE on the local system. It is launched from a shell.
Splunk Web	Splunk Web (or "Web GUI") is a web-based application that can be used to manage the TOE remotely using HTTPS.
User	An individual who has access to the TOE but is not able to manage its behavior.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Splunk Enterprise 6.4.5 Security Target, version 1.0, dated January 20, 2017
6. Splunk® Enterprise Securing Splunk Enterprise with Common Criteria 6.4.5