National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Splunk Enterprise 9.0.4

Report Number: CCEVS-VR-VID11330-2023
Version: 1.0
Date: March 23, 2023

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant
Lauren Hardy
Lisa Mitchell
Clare Parran

The MITRE Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Evan Seiz
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

List of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Splunk Enterprise 9.0.4 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 (TOE) 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 Laurel, Maryland, United States of America, and was completed in March 2023. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) 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 1.4* (APP_PP), Oct 18, 2021 and the *Functional Package for Transport Layer Security, Version 1.1* (TLS_PKG), March 01, 2019.

The TOE is the Splunk Enterprise 9.0.4 ("Splunk") application executing on a Linux operating system (OS). The primary function of Splunk is to collect system generated data from various types of platform systems and aggregate it in a centralized location for real-time visibility and analysis of system behavior. Additional operational functional behavior is dependent on whether the TOE has been configured to be used as an indexer or a forwarder.

The indexer functionality is responsible for receiving data from trusted external sources such as databases, web services, and one or more additional instances of Splunk configured with the forwarder functionality enabled via HTTPS/TLS. Whereas the forwarder functionality is responsible for transmitting the system-generated data to an external trusted entity, such as an additional instance of Splunk configured with the indexer functionality enabled via HTTPS/TLS.

While the product vendor provides multiple versions of the product, only the full Linux version of Splunk Enterprise 9.0.4, operating on Red Hat Enterprise Linux (RHEL) and configured with either the indexer or the forwarder functionality enabled, is considered the TOE – other product versions or platforms were not evaluated, and no security claims are made for them. In the evaluated configuration, Splunk Enterprise 9.0.4 is installed on top of the RHEL OS. When the TOE is configured with the indexer functionality (aka Splunk indexer), any Splunk forwarders are considered to be trusted non-TOE external transmitters (data feeds). When the TOE is configured with the forwarder functionality (aka Splunk forwarder), then the receiving Splunk indexer is considered to be a trusted non-TOE external data feed receiver.

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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the APP_PP. 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 individual work units of the ETR for the APP_PP Assurance Activities. The Validation team found that the evaluation showed that the product satisfies all of 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Splunk Enterprise 9.0.4 Security Target v1.0*, dated March 15, 2023 and analysis performed by the Validation Team.

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 Profile containing Assurance Activities, which are interpretation 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 Compliant List.

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

- The TOE: the fully qualified identifier of the product as evaluated.
- The 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.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Splunk Enterprise 9.0.4
Protection Profile	Protection Profile for Application Software Version 1.4 [APP_PP], Functional Package for Transport Layer Security, Version 1.1 [TLS_PKG], including all applicable NIAP Technical Decisions and Policy Letters
Security Target	Splunk Enterprise 9.0.4 Security Target v1.0 dated March 15, 2023
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Splunk Incorporated Splunk Enterprise 9.0.4" Evaluation Technical Report v1.0 dated March 15, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Splunk Inc.
Developer	Splunk Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Sheldon Durrant, Lauren Hardy, Lisa Mitchell, Clare Parran

Table 1: Evaluation Identifiers

3 Assumptions and Clarification of Scope

3.1 Assumptions

The assumptions are drawn directly from the APP_PP.

3.2 Threats

The threats are drawn directly from the APP_PP.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. 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 1.4* and *Functional Package for Transport Layer Security, Version 1.1*, including all relevant NIAP Technical Decisions. A subset of the “optional” and “selection-based” security requirements defined in the APP_PP and TLS_PKG are claimed by the TOE and documented in the ST.
- This evaluation covers only the specific device model and software version identified in this document, and not any earlier or later versions released or in process.
- 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 Security Target. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the Splunk Enterprise 9.0.4 support for collecting system-generated data from the general-purpose computer that it resides on and receiving data feeds from external sources such as databases, web services, and one or more additional instances of Splunk configured as a forwarder, described in Section 1.3 of the Security Target were not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

4 Architectural Information

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

4.1 TOE Introduction

The TOE type for Splunk Enterprise 9.0.4, configured as either an indexer or forwarder, is Application Software. The Protection Profile for Application Software (App PP) specifies several use cases that conformant TOEs may implement. In particular the TOE supports:
Use Case 1, Content Creation is defined as follows: “The application allows a user to create content, saving it to either local or remote storage. Example content includes text documents, presentations, and images.”

> Splunk indexer implicitly supports a user’s ability to create content by creating/collecting system data from its host platform and storing it locally in a datastore (indexes) for the end user consumption.
>
> Splunk forwarder implicitly supports a user’s ability to create content by creating/collecting system data from its host platform and storing it remotely, to such a device as a Splunk indexer, for the end user consumption.

Use Case 2, Content Consumption, is defined as follows: “The application allows a user to consume content, retrieving it from either local or remote storage.”

> Splunk indexer is considered to implement content consumption because it allows a user to consume (query) system data stored on the local filesystem (indexes) and generate human-readable reports and views on this data.

4.2 Physical Boundary

Splunk Enterprise 9.0.4 is a software-only TOE. All hardware that is present is part of the TOE’s Operational Environment. The following system configurations were used for the testing of the TOE:

- Configuration 1:
  - Red Hat Enterprise Linux 8.2 64 bit
  - Intel(R) Xeon(R) CPU E5-2630v4
  - 16 GB RAM
  - 500 GB disk
- Configuration 2:
  - Red Hat Enterprise Linux 7.9 64 bit
  - Intel(R) Xeon(R) CPU E5-2630v4
  - 16 GB RAM
  - 500 GB disk

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
External Trusted Data Feed	External data source for transmitting non-TSF related data to the TOE indexer for populating Splunk’s datastore (indexes). The external data source must use HTTPS/TLS to communicate with the TOE.

External Trusted Data Feed Receiver	External data source for receiving non-TSF related data from the TOE forwarder. The external data source must use HTTPS/TLS to communicate with the TOE.
Host Platform	A general-purpose computer on which the Linux operating system and the TOE is installed. The TOE requires network resources from the host platform. Note that the host platform can also be used to administer the TOE locally.
Management Workstation	Any general-purpose computer that is used by a security administrator to manage the TOE remotely via a web browser.
SMTP Server	An email server that can receive alerts from the TOE and deliver them to users in the Operational Environment via email.
CRL Distribution Point	A server that provides updated revocation lists for the TOE’s certificate validation functionality.

Table 2: IT Environment Components

5 Security Policy

5.1 Cryptographic Support

The TOE software includes OpenSSL which performs the TOE's cryptographic operations required to support the establishment of trusted channels and paths to protect data in transit. 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).
The following table contains the CAVP algorithm certificates:

SFR	Cert Name (Claimed Algorithm)	CAVP Cert. #
FCS_CKM.1 Key generation	ECDSA: 186-4 Key Pair Generation and Private Key Validation (P-256, P-384, P-521)	A2913
FCS_CKM.1/AK Asymmetric key generation	ECDSA: 186-4 Key Pair Generation and Private Key Validation (P-256, P-384, P-521)	A2913
FCS_CKM.2 Key establishment	ECDHE: KAS-ECC (P-256, P-384, P-521)	A2913
FCS_COP.1/SKC Encryption/decryption	AES (CBC-256, GCM-128, GCM-256, CTR-256)	A2913
FCS_COP.1/Hash Hash	SHS (SHA-256, SHA-384, SHA-512)	A2913
FCS_COP.1/Sig Signing and verification	ECDSA: Signature Generation and Signature Verification (P-256: SHA-256, SHA-384, SHA512 P-384: SHA-256, SHA-384, SHA512 P-521: SHA-256, SHA-384, SHA512)	A2913
FCS_COP.1/KeyedHash Keyed-hash message authentication	HMAC (HMAC-SHA-256, HMAC-SHA-384)	A2913
FCS_RBG_EXT.1 Random Bit Generation	DRBG (CTR-DRBG) requires AES-CTR 256 bit	A2913

Table 3: Cryptographic Algorithm Table (OpenSSL)

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 only requires the use of the underlying platform's network connectivity for administrative activities, email alerts, receipt and transmission of non-TSF related data from/to external trusted data feeds.

5.3 Identification and Authentication

In order to facilitate secure communications using HTTPS/TLS, the TOE provides a mechanism to validate X.509 certificates. While the HTTPS/TLS implementation will automatically reject a certificate if it is found to be invalid, a certificate with unknown revocation status is accepted.

5.4 Security Management

The TOE does not provide any default credentials for use with initial authentication and requires the security administrator to define their username and password during installation. 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 uses the underlying platform’s recommended methods for storing and setting configuration options. The TOE also provides the security administrators with the ability to configure the supported TLS cipher suites of the trusted channels and query the existing TOE software version.

5.5 Privacy

The TOE ensures the privacy of its security 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 not allocating any memory region with both write and execute permissions. The TOE is also compatible with SELinux and is built 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. The TOE is also versioned with SWID tags. The TOE’s initial installation package and software updates must be manually downloaded to the platform’s file system and installed using the platform’s package manager. In the evaluated configuration, the security 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 the TOE package prior to installation.

5.7 Trusted Path/Channel

The TOE protects all data in transit using HTTPS over TLS or standalone TLS. HTTPS/TLS protocol is used to secure remote administration using the web UI. The TOE, acting as an indexer, uses TLS to securely send alerts to a remote SMTP server in the Operational Environment. HTTPS/TLS is used to secure communications between the TOE operating as an indexer and external trusted data feeds. Additionally, the TOE operating as a forwarder requires the use of HTTPS/TLS to secure communications for transmitting data to an external trusts data feed receiver.

6 Documentation

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

- Splunk Enterprise 9.0.4 Supplemental Administrative Guidance for Common Criteria – v1.0, March 15, 2023

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 Evaluated Configuration

The TOE is the Splunk Enterprise 9.0.4 ("Splunk") application executing on a Linux OS. In the evaluated configuration, Splunk Enterprise 9.0.4 is installed on top of the RHEL OS (8.2 and 7.9) and configured with either the indexer or forwarder functionality enabled. The administrative interfaces include a local CLI and a web UI for remote access. The TOE is configured to securely communicate with the following external IT entities: SMTP server (transmitting only) and external trusted data feed (receiving and transmitting). All claimed PP related functionality is contained whether Splunk is configured as an indexer or a forwarder.

Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- External Trusted Data Feed
- External Trusted Data Feed Receiver
- Host Platform
- Management Workstation
- SMTP Server
- CRL Distribution Point

To use the product in the evaluated configuration, the product must be configured as specified in the *Splunk Enterprise 9.0.4 Supplemental Administrative Guidance for Common Criteria Version 1.0, March 15, 2023* 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 *Splunk Incorporated Splunk Enterprise 9.0.4 Evaluation Technical Report v1.0 dated March 15, 2023*, as summarized in the publicly available *Assurance Activity Report for a Target of Evaluation "Splunk Enterprise 9.0.4" Assurance Activities Report v1.0, March 15, 2023*.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The test team's test approach was to 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 testing assurance activities as defined by the APP_PP for all *security relevant* TOE external interfaces. TOE external interfaces that will be 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 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.

8.3 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the APP_PP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
Splunk	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
Splunk Enterprise (Version 9.0.4)	This is a generic term for searching for known vulnerabilities for the specific product. In this case Splunk would find the vulnerability and Enterprise would be used to narrow the list to a specific software product and version.
OpenSSL (1.0.2zf-fips)	Provides all of the security encryption functionality required by Splunk
Declared library list from FPT_LIB_EXT.1	

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources (updated March 15, 2023). The following public vulnerability sources were searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- g) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- h) Offensive Security Exploit Database: https://www.exploit-db.com/

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. Testing that was conducted under the functional testing that would have been duplication of a vulnerability tests were not re-run. This left one remaining exploit to further explore: malicious binary.

The team tested the following areas:

- Burp Suite Scan
  - Perform security testing of web applications
- Virus/Malware Scan
  - Perform a virus scan on software as required by the APP_PP assurance activity requirements.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

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 5 and CEM version 3.1 Rev 5. 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 and TLS_PKG.

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. The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

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 9.0.4 product that is 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 and TLS_PKG in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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 and TLS_PKG related to the examination of the information contained in the TOE Summary Specification.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

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 and TLS_PKG related to the examination of the information contained in the operational guidance documents.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

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.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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 Assurance Activities in the APP_PP and TLS_PKG. The lab recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the APP_PP and TLS_PKG, and that the conclusion reached by the Evaluation team was justified.

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.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the APP_PP and TLS_PKG, and that the conclusion reached by the Evaluation team was justified.

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 TLS_PKG, 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 9.0.4 Supplemental Administrative Guidance for Common Criteria Version 1.0, March 15, 2023* document. The product vendor provides multiple versions of the product, only the full Linux version of Splunk Enterprise 9.0.4, operating on 8.2 and 7.9 versions of Red Hat Enterprise Linux (RHEL) and configured with either the indexer or forwarder functionality enabled, is considered to be the TOE – other product versions or platforms were not evaluated and no security claims are made for them.

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.

Consumers employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Splunk Enterprise 9.0.4 Security Target v1.0,* dated March 15, 2023.

13 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ASLR	Address Space Layout Randomization
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
CRL	Certificate Revocation List
DHE	Diffie-Hellman Key Exchange
DRBG	Deterministic Random Bit Generator
ECDHE	Elliptic Curve Diffie-Hellman Key Exchange
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galois/Counter Mode
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
JIT	Just-in-Time (compilation)
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
NIAP	National Information Assurance Partnership
RBG	Random Bit Generator
RHEL	Red Hat Enterprise Linux
SAR	Security Assurance Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

Table 4: Acronyms

14 Terminology

Term	Definition
Security Administrator	A security 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.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a security administrator uses to manage it (web browser, terminal client, etc.).
User	An individual who has access to the TOE but is not able to manage its behavior.

Table 5: Terminology

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Protection Profile for Application Software Version 1.4.
6. Functional Package for Transport Layer Security, Version 1.1.
7. Splunk Enterprise 9.0.4 Security Target v1.0, dated March 15, 2023.
8. Splunk Enterprise 9.0.4 Supplemental Administrative Guidance for Common Criteria Version 1.0, dated March 15, 2023.
9. Assurance Activity Report for a Target of Evaluation Splunk Enterprise 9.0.4 Assurance Activities Report v1.0 dated March 15, 2023.
10. Splunk Incorporated Splunk Enterprise 9.0.4 Evaluation Technical Report v1.0 dated March 15, 2023.