National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Nessus Agent 10.4.1

Report Number: CCEVS-VR-VID11367-2023
Dated: 7/7/2023
Version: 1.0

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

Russell Fink

Seada Mohammed

Jerome Myers

Marybeth Panock

Michael Smeltzer

Common Criteria Testing Laboratory

Leidos Inc.

Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Nessus Agent 10.4.1, supported on RHEL 8.7 and Windows Server 2019 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in July 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the following document:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
- *Functional Package for Transport Layer Security* (TLS), Version 1.1, 1 March 2019 ([11])

The TOE is Nessus Agent 10.4.1, supported on RHEL 8.7 and Windows Server 2019.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile, and when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([6]).

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 (PCL).

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

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules 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	Nessus Agent 10.4.1, supported on RHEL 8.7 and Windows Server 2019
Security Target	Nessus Agent 10.4.1 Security Target, Version 1.1, 28 June 2023
Sponsor & Developer	Tenable, Inc. 6100 Merriweather Drive 12th Floor Columbia, MD 21044
Completion Date	TBD
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5]) *Functional Package for Transport Layer Security* (TLS), Version 1.1, 1 March 2019 ([11])
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Armin Najafabadi Greg Beaver Pascal Patin Srilekha Vangala
Validation Personnel	Russell Fink Seada Mohammed Jerome Myers Marybeth Panock Michael Smeltzer

3 TOE Architecture

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

The Nessus Agent 10.4.1 TOE is a software application that runs on the following platforms:

- RHEL 8.7
- Windows Server 2019.

The product architecture is depicted in the following figure. The Nessus Agent application (the TOE) is indicated by the blue box. Figure 1 shows the TOE in a sample deployment with other Tenable applications in its operational environment.

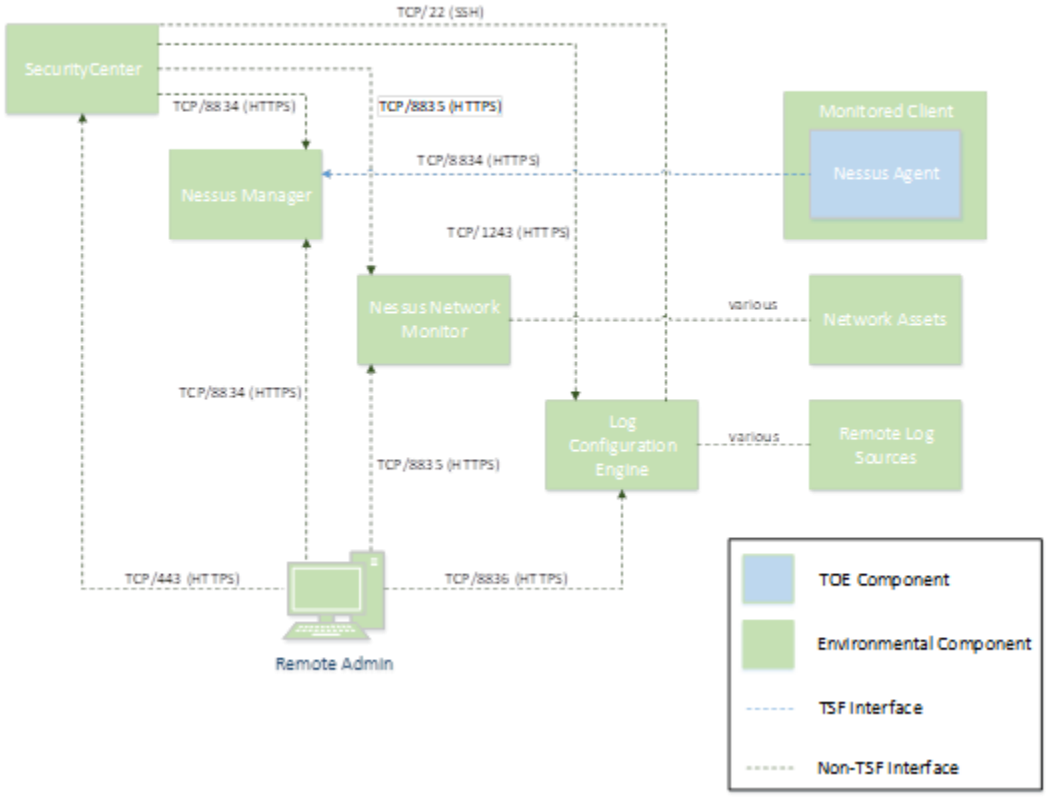


Figure 1: Nessus Agent 10.4.1 Architecture

TSF-relevant remote interfaces are shown in Figure 1. Note that the TOE consists of exactly one instance of Nessus Agent. However, it is expected that in a typical deployment, many instances of the Nessus Agent application will be deployed on organizational systems. This does not affect the security claims made by the TOE because there is no direct interface from one instance of Nessus Agent to another.

The TOE has the following minimum system requirements for its host platform:

- 1x dual-core CPU (any dual-core CPU's clock speed is sufficient)
- 1 GB RAM
- 2 GB disk storage

- 15-50 IOPS disk speed.

These system requirements reflect the lightest usage scenarios for the TOE. Additional factors such as network size and storage retention requirements will affect the system requirements for a particular deployment.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Timely Security Updates

The TOE developer has internal mechanisms for receiving reports of security flaws, tracking product vulnerabilities, and distributing software updates to customers in a timely manner.

4.2 Cryptographic Support

The TOE implements cryptography to protect data in transit. The TOE does not store credential data on the local system so no separate data at rest protection mechanism is implemented.

For data in transit, the TOE implements TLS/HTTPS as a client to communicate with an instance of Nessus Manager in the operational environment. The TOE's TLS client does not support mutual authentication.

The TOE implements all cryptography used for this function using its own implementations of OpenSSL with NIST-approved algorithms. The TOE's DRBG is seeded using entropy from the underlying OS platform.

4.3 User Data Protection

The TOE is compatible with the use of platform full disk encryption to protect sensitive data at rest.

The TOE relies on the network connectivity and system log capabilities of its host OS platform. The TOE supports application-initiated uses of the network. The TOE also accesses various system resources as part of conducting system scans. Specifically, the TOE supports local scanning of the system that it is installed on.

4.4 Identification and Authentication

The TOE supports X.509 certificate validation as part of establishing TLS and HTTPS connections. The TOE supports various certificate validity checking methods and can also check certificate revocation status using OCSP. If the validity status of a certificate cannot be determined, the certificate will be accepted. All other cases where a certificate is found to be invalid will result in rejection without an administrative override.

4.5 Security Management

Both the TOE binary components themselves and the configuration settings they use are stored in locations recommended by the platform vendors.

The TOE does not include a direct user interface to manage its functionality. Security-relevant configuration of the TOE is initiated from the Nessus Manager application in the TOE's operational environment. This configuration relates to the circumstances under which the TOE will transmit data about the local system's hardware, software, and configuration information (i.e., scan results) back to its operational environment.

4.6 Privacy

The TOE does not handle personally identifiable information (PII) of any individuals.

4.7 Protection of the TSF

The TOE enforces various mechanisms to prevent itself from being used as an attack vector to its host OS platform. Each TOE platform version (Windows and Linux) implements address space layout randomization (ASLR), does not allocate any memory with both write and execute permissions, does not write user-modifiable files to directories that contain executable files, is compiled using stack overflow protection, and is compatible with the security features of its host OS platform.

Each TOE platform version contains libraries and invokes system APIs that are well-known and explicitly identified.

The TOE has a mechanism to determine its current software version. Software updates to the TOE can be acquired by leveraging its OS platform or through its connection with the environmental Nessus Manager application. The format of the software update is dependent on the TOE platform version. All updates are digitally signed to guarantee their authenticity and integrity.

4.8 Trusted Path/Channels

The TOE encrypts sensitive data in transit between itself and its operational environment using TLS and HTTPS.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

5.2 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 shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following document:
  - *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
  - *Functional Package for Transport Layer Security* (TLS), Version 1.1, 1 March 2019 ([11])
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in *Nessus Agent 10.4.1 Security Target*, Version 1.1, 28 June2023 ([6]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives 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 TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Nessus Agent 10.4.x User Guide, Last Updated: May 19, 2023* ([7]).

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

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 TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Nessus Agent 10.4.1 Common Criteria Test Report and Procedures,* Version 1.1, June 28, 2023 [10]

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report For Nessus Agent 10.4.1, Version 1.1, June 28, 2023* ([9])

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specification:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021
- *Functional Package for Transport Layer Security* (TLS), Version 1.1, 1 March 2019.

The evaluation team devised a test plan based on the test activities specified in the PP. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above.

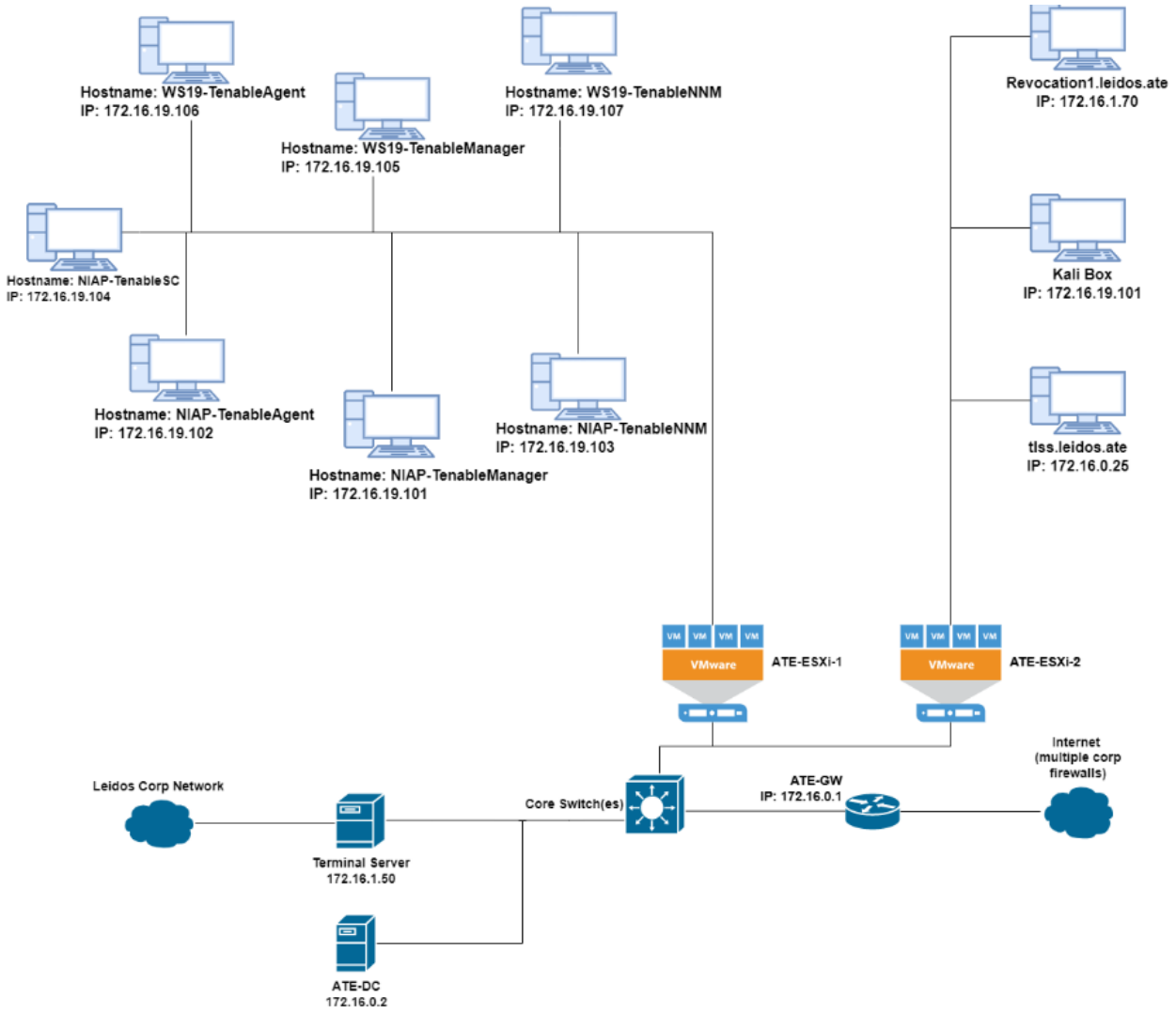
Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from October 2022 to June 2023.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the team test plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Application Software* were fulfilled.

7.1 Test Configuration

This section identifies the devices used for testing the TOE and describes the test configuration. The test configuration is described below:



As documented in the diagram above, the following hardware and software components were included in the evaluated configuration during testing:

TOE

- NIAP-TenableAgent
  - Platform: Red Hat Enterprise Linux 8.7
  - IP:172.16.19.102
  - Running on ATE-ESXi-1 (VMware ESXi, 6.5.0)
    - CPU: AMD Ryzen Threadripper 1950X 16-Core Processor
- WS19-TenableAgent
  - Platform: Windows Server 2019
  - IP: 172.16.19.106
  - Running on ATE-ESXi-1 (VMware ESXi, 6.5.0)
    - CPU: AMD Ryzen Threadripper 1950X 16-Core Processor
- NIAP-TenableManager
  - Platform: Red Hat Enterprise Linux 8.7

    - IP: 172.16.19.101
    - Running on ATE-ESXi-1 (VMware ESXi, 6.5.0)
        - CPU: AMD Ryzen Threadripper 1950X 16-Core Processor
- WS19-TenableManager
    - Platform: Windows Server 2019
    - IP: 172.16.19.105
    - Running on ATE-ESXi-1 (VMware ESXi, 6.5.0)
        - CPU: AMD Ryzen Threadripper 1950X 16-Core Processor
- NIAP-TenableNNM
    - Platform: Red Hat Enterprise LInux 8.7
    - IP: 172.16.19.103
    - Running on ATE-ESXi-1 (VMware ESXi, 6.5.0)
        - CPU: AMD Ryzen Threadripper 1950X 16-Core Processor
- WS19-TenableNNM
    - Platform: Windows Server 2019
    - IP: 172.16.19.107
    - Running on ATE-ESXi-1 (VMware ESXi, 6.5.0)
        - CPU: AMD Ryzen Threadripper 1950X 16-Core Processor

Additional Components

ATE-GW (Physical)
Purpose: Main router/gateway
IP/MASK/MAC: 172.16.0.1 / 16 / ac:1f:6b:95:0c:1d
OS: PfSense 2.4.4-RELEASE-p2

ATE-DC (Physical)
Purpose: Main Domain Controller (DC) for Test environment/DNS server
IP/MASK/MAC: 172.16.0.2 / 16 / 00:22:19:58:EB:8D
OS: Windows Server 2016 version 1607
Protocols used: RDP, NTP, LDAP, DNS

ATE-ESXi-1 (Physical)
Purpose: Virtualization server
IP/MASK/MAC: 172.16.1.62 / 16 / 10:7b:44:92:77:bf
OS: VMware ESXi, 6.5.0, 5969303

ATE-ESXi-2 (Physical)
Purpose: Virtualization server
IP/MASK/MAC: 172.16.1.63 / 16 / ac:1f:6b:c6:50:96
CPU: Intel(R) Xeon(R) Gold 6248 CPU @ 2.50GHz
OS: VMware ESXi, 6.7.0, 13006603

Terminal Server
Purpose: Provide tester access to the Test Environment from corporate network.
IP/MASK/MAC: 172.16.1.50 / 16 / D4:BE:D9:B4:FE:66
OS: Windows server 2016 version 1607
Protocols used: RDP, NTP, LDAP, DNS, SSH

Revocation1.leidos.ate (VM)
Purpose: Hosts TLS/OCSP Test Tools
IP/MASK/MAC: 172.16.1.70/ 16 / 00:50:56:b1:a0:fd
OS: Ubuntu 18.04.4

Protocols Used: SSH, TLS, OCSP
Running on ATE-ESXi-2 (VMware ESXi, 6.7.0, 13006603)
Relevant Software:
OpenSSL 1.1.1
Wireshark 2.6.10

TLSS.leidos.ate (VM)
Purpose: Hosts TLS Test Tools
IP/MASK/MAC: 172.16.0.25 / 16 / 00:50:56:b1:66:0b
OS: Ubuntu 18.04.5
Protocols Used: SSH, TLS, NTP, DNS
Running on ATE-ESXi-2 (VMware ESXi, 6.7.0, 13006603)
Relevant Software:
Proprietary Python TLS test tools
OpenSSL 1.1.1
Wireshark 2.6.10

Kali Box (VM)
Purpose: Hosts TLS Test Tools
IP/MASK/MAC: 172.16.0.161 / 16 / 00:50:56:b1:60:37
OS: Kali 2019.3
Protocols Used: SSH,
Running on ATE-ESXi-1 (VMware ESXi, 6.5.0)
CPU: AMD Ryzen Threadripper 1950X 16-Core Processor
Relevant Software:
SSLyze v2.0.6
OpenSSL 1.1.1

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is the Nessus Agent 10.4.1, supported on RHEL 8.7 and Windows Server 2019.

Nessus Agent 10.4.1 (Nessus Agent) is a software product designed to be installed on an endpoint system to facilitate local scanning of that system. Local scanning allows Nessus Agent to collect detailed information about the system's hardware, software, and configuration, which can be used to determine compliance with organizational security policies and whether potential exploitable vulnerabilities are present on that system.

Nessus Agent is deployed and configured by an environmental instance of Nessus, which also collects scan results from Nessus Agent for aggregation and analysis. Nessus in turn will transmit this data to an environmental instance of Tenable.sc (SecurityCenter), where it can be combined with network traffic and system log data to provide a comprehensive window into the security posture of an organization.

The TOE is capable of running on a general-purpose Windows or Linux operating system on standard consumer-grade hardware on either a physical or virtual machine. For the evaluated configuration, the TOE was tested on virtualized instances of Windows Server 2019 and RHEL 8.7, each running on VMware ESXi 6.5 on a system using an AMD Ryzen Threadripper 1950X processor with the Zen microarchitecture.

8.2 Excluded Functionality

Excluded Functionality
The TOE's scanning and data collection capabilities are outside the scope of the TOE (aside from the trusted channel used to transmit the collected data), as is any other product behavior that is not described in [APP_PP] or [TLS_PKG]. The content and execution of plugins is similarly excluded from the TOE, although they are discussed in the context of network communications because the TSF must use platform network resources to acquire them.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary *Evaluation Technical Report For Nessus Agent 10.4.1*, Part 2 (Leidos Proprietary) Version 1.0, June 1, 2023 ([8]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
- Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 ([11]).

The evaluation determined the TOE satisfies the conformance claims made in the Nessus Agent 10.4.1 Security Target, Version 1.1, 28 June 2023, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the PP listed above.

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

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the following public vulnerability databases:

- National Vulnerability Database (https://nvd.nist.gov/)
- Tenable CVEs: (https://www.tenable.com/cve)
- OpenSSL Vulnerabilities: (https://www.openssl.org/news/vulnerabilities-3.0.html)
- Carnegie Mellon University CERT Coordination Center https://www.kb.cert.org/vuls/search/

Searches were performed on 4 April 2023 and updated on 22 May 2023 using the following search terms:

- “tenable”
- “nessus”
- “tls v1.2”
- “openssl 3.0.9”
- Third-Party Libraries

  Listed below are the third-party libraries used by the TOE. Note that these libraries do not necessarily relate to the TOE functionality claimed in the Security Target; however, since they are bundled with the product itself they are disclosed since a vulnerability in outside the logical boundary of the product could still present an exploitable vulnerability.

Plugin Name	Agent 10.4.1
apr-iconv	1.2.2
ced	Commit 1193457d
expat	2.5.0
jemalloc	5.2.1
libbzip2	1.0.8
libpcre	8.42
libjpeg	9d
libxml2	2.10.3
libxslt	1.1.34
libxmlsec	1.2.25
zlib	1.2.13
openssl	3.0.9

sqlite	3.34.1
jsonsl	Commit 684b60f
Snappy	1.1.7
RapidJSON	1.1.0
MS VC Redist	14.22

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. Additionally, the evaluation team's testing 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 followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

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

Consumers should also note that the TOE is an agent installed on endpoint system in order to conduct security scanning. The information it collects is sent back to a management server over TLS. It does not have any kind of management functionality aside from the ability to connect it to a management server. All other management is done by the management server.

11 Security Target

The ST for this product's evaluation is *Nessus Agent 10.4.1 Security Target, Version 1.0, 18 May 2023* ([6]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Application Software, Version 1.4, 07 October 2021.

[6] Nessus Agent 10.4.1 Security Target, Version 1.1, 28 June 2023.

[7] Nessus Agent 10.4.x User Guide, Last Updated: May 19, 2023.

[8] Evaluation Technical Report For Nessus Agent 10.4.1, Part 2 (Leidos Proprietary) Version 1.1, June 28, 2023.

[9] Assurance Activities Report For Nessus Agent 10.4.1, Version 1.1, June 28, 2023.

[10] Nessus Agent 10.4.1 Common Criteria Test Report and Procedures, Version 1.1, June 28, 2023.

[11] Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019