National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Nessus Manager 8.11.1

Report Number:	**CCEVS-VR-VID11067-2020**
Dated:	**8 December 2020**
Version:	**1.0**

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

<u>Validation Team</u>

Jerome F. Myers, PhD

Marybeth Panock

The Aerospace Corporation

<u>Common Criteria Testing Laboratory</u>

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Nessus Manager 8.11.1 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This Validation Report (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.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in December 2020. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos. The evaluation determined that the TOE is:

- Common Criteria Part 2 Extended and Part 3 Conformant

and demonstrates exact conformance to:

- *Protection Profile for Application Software*, Version 1.3, 1 March 2019 [5]
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 [6]

as clarified by all applicable Technical Decisions.

The TOE is Nessus Manager 8.11.1, supported on Red Hat Enterprise Linux (RHEL) 7 and Windows Server 2016.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory (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). 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 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 Evaluation Technical Report (ETR) and the Assurance Activities Report (AAR). 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). The conclusions of the testing laboratory in the evaluation technical report 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 product meets the Common Criteria requirements of the Protection Profile for Application Software, Version 1.3, 1 March 2019 and the Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019. The technical information included in this report was obtained from the *Nessus Manager 8.11.1 Security Target*, Version 1.0, 4 December 2020 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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria 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 Target of Evaluation (TOE)—the fully qualified identifier of the product as evaluated
- The Security Target (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 Manager 8.11.1
Protection Profiles	• Protection Profile for Application Software, Version 1.3, 1 March 2019 • Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019
Security Target	Nessus Manager 8.11.1 Security Target, Version 1.0, 4 December 2020
Evaluation Technical Report	• Evaluation Technical Report for Tenable Nessus Manager 8.11.1, Part 1 (Leidos Non-Proprietary), Version 1.1, 4 December 2020 Evaluation Technical Report for Tenable Nessus Manager8.11.1, Part 2 (Leidos Proprietary), Version 1.1, 4 December 2020.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Tenable, Inc.
Developer	Tenable, Inc.
Common Criteria Testing Laboratory (CCTL)	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive

Item	Identifier
	Columbia, MD 21046
Validation Personnel	Jerome F. Myers, PhD Marybeth Panock

3 TOE Architecture

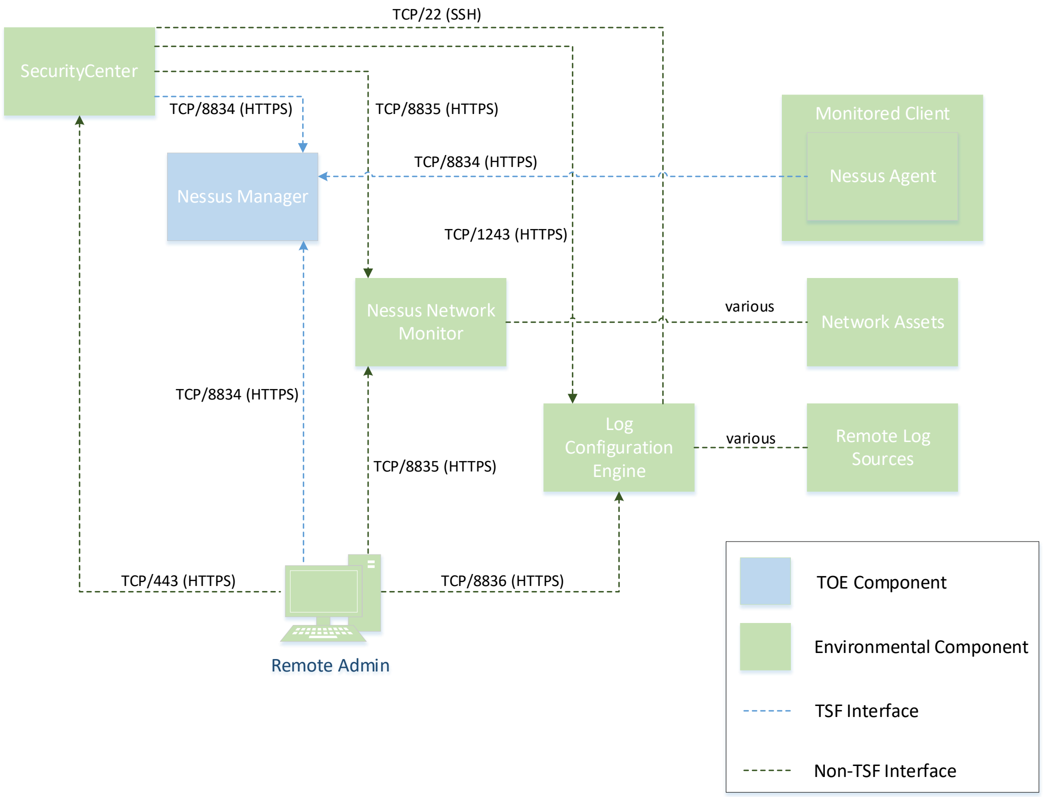
Note: The following architectural description is based on the description presented in the Security Target.

Nessus Manager is a vulnerability management product that is designed to provide visibility into system assets. The product is used to discover and scan assets such as servers, endpoints, network devices, operating systems, databases, and applications. It can do this on its own through remote scanning. However, Nessus Manager can also be used to deploy, configure, and collect data from environmental Nessus Agent applications that are installed on endpoint systems to collect more detailed system data through local scanning. Regardless of how it is obtained, information collected by Nessus Manager can be fed to the environmental Tenable.sc product for centralized aggregation, analysis, and reaction.

Nessus Manager is the same application as Nessus, which is also developed by Tenable. The additional features that Nessus Manager provides are activated by licensing. The primary difference between Nessus and Nessus Manager is that Nessus Manager has the ability to configure, manage, and collect data from Nessus Agents, whereas Nessus can only perform agentless remote scanning.

The TOE consists of the Nessus Manager application, which is a C/C++ application with a PHP/JavaScript web front-end running on a proprietary web server. The TOE has both Linux and Windows platform versions. The following figure depicts a sample deployment of the TOE with other Tenable applications in its operational environment.

Figure 1 – Example Deployment



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

- 4 x 2GHz cores
- 16 GB RAM
- 30 GB disk storage (direct-attached storage required).

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. Refer to the relevant Guidance Section (as referenced in Section 7 Documentation) for the specific system requirements that apply to a given deployment.

There are no fixed network ports that must always be open for the TOE to function. Some network ports must be open, but these are configurable if the default ports cannot be used. The connections and their default ports are as follows:

- TCP/8834 (for administrator communications, communications with Tenable.sc, and communications with Nessus Agents)

Nessus Manager will perform unauthenticated remote scans against target systems on various ports to determine whether services are available on those systems. This functionality is not within the scope of the TOE because it is not "sensitive data" but it is necessary for the product to function as advertised. In particular, if network configuration between Nessus and a target system blocks traffic to that system, it may result in a false negative if a service is actually running on the target system but cannot be detected by Nessus because of network configuration. The remote scan may also require Nessus Manager to invoke the OS platform's SSH client to communicate with a remote system using SSH. This is not a TSF interface so it is outside the scope of this ST.

The TOE's operational environment includes the following:

- An instance of Tenable.sc and one or more instances of Nessus Agent applications (other Tenable components—Nessus Manager and Log Correlation Engine—are expected to be present in the TOE's operational environment because they also interface with Tenable.sc, but the TOE does not interact with these applications directly).
- Platform (hardware and software) on which the TOE is hosted.
  - 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 2016 and RHEL 7, each running on VMware ESXi 6.5 on a system using an AMD Ryzen Threadripper 1950X processor with the Zen microarchitecture.
- Full disk encryption is required for the TOE platform to ensure adequate data-at-rest protection.
- Web browser used to access the GUI interface.

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 at rest and in transit.

For data at rest, the TOE stores credential data used to log in to the TOE as well as passphrase data used to protect PKI certificates that the TOE uses to authenticate to environmental components. This stored data is encrypted using AES or a PBKDF, depending on the data that is being stored.

For data in transit, the TOE implements TLS/HTTPS as a server. The TOE implements a TLS server for its administrative interface and to receive communications from other Tenable components in the operational environment.

The TOE implements all cryptography used for these functions 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 uses cryptographic mechanisms to protect sensitive data at rest. The key used by the TOE to encrypt and decrypt sensitive data is cryptographically protected by the TOE platform.

The TOE relies on the network connectivity and system log capabilities of its host OS platform. The TOE supports user-initiated, externally-initiated, and application-initiated uses of the network. The TOE also access various system resources as part of conducting system scans. Specifically, the TOE supports remote scanning of a variety of target host systems from network devices to PCs running general-purpose operating systems. For the target system, the TOE can examine externally-visible ports and services. If provided credentials (either by receiving them from Tenable.sc or by direct administrator input), the TOE can authenticate to the target system and utilize platform specific tools such as apt, yum, and WMI to collect more detailed information about the system.

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

The TOE itself and the configuration settings it uses are stored in locations recommended by the platform vendor for both Windows and Linux application versions.

The TOE includes a web GUI. This interface enforces username/password authentication using locally-stored credentials that are created using the TOE. The TOE does not include a default user account to access its management interface.

The security-relevant management functions supported by the TOE relate to configuration of transmission of system data (through execution of remote scanning) and configuration of transmission of application state information.

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. 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. It facilitates the transmission of sensitive data from remote users over TLS and HTTPS.

5 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.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that may benefit from need 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 evaluation activities specified in *Protection Profile for Application Software*, Version 1.3, 1 March 2019 [5] and in *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 [6], and performed by the evaluation team).
- 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 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality listed in Section 9.2 of this document is not covered.

7 Documentation

Tenable 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 model is as follows:

- Nessus 8.11.x User Guide, Last Revised: October 29, 2020.

To use the product in the evaluated configuration, the product must be configured as specified in the sub-section “Configure Nessus for NIAP Compliance” found within this guide.

The documentation listed above is the only documentation that should be trusted to install, administer, or use the TOE in its evaluated configuration. 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. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. The information is derived from the Evaluation Technical Report for Tenable Nessus Manager 8.11.1 Part 2 (Leidos Proprietary), Version 1.1, 4 December 2020 [ETR Prop-P2] and the test report, Tenable Nessus Manager 8.11.1 *Common Criteria Test Report and Procedures*, Version 1.1, 4 December 2020 [12], which are listed in the bibliography section 14 of this document. A non-proprietary description of the tests performed, and their results is provided in the *Assurance Activities Report for Nessus Manager 8.11.1*, Version 1.1, 4 December 2020 [11].

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

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 *Protection Profile for Application Software* ([5]) and *Functional Package for Transport Layer Security (TLS)* ([6]).

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Application Software* and *Functional Package for Transport Layer Security (TLS)*. 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. Testing occurred from February 3, 2020 to October 23, 2020; testing was completed in October 2020.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the vendor-provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory. The Independent Testing activity is documented in the Assurance Activities Report (AAR), which is publicly available, and is not duplicated here. A description of the test configurations and the test tools may be found in Section 2.8 of that report.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Application Software* and *Functional Package for Transport Layer Security (TLS)* were fulfilled.

8.3 Test Configuration

The evaluation team established a test configuration comprising:

- TOE components:
  - Nessus Manager 8.11.1, running on Red Hat Enterprise Linux (RHEL) 7.7. RHEL itself was running on ESXi 6.5 on AMD Ryzen Threadripper 1950X (Zen)
  - Nessus Manager 8.11.1, running on Windows Server 2016 Standard. Windows Server itself was running on ESXi 6.5 on AMD Ryzen Threadripper 1950X (Zen)
- Operational and test environment components:
  - Tenable.sc 5.15.0 on Linux RHEL 7.7
  - Nessus Agent 8.0.0 on Linux RHEL 7.7

- Nessus Agent 8.0.0 on Windows Server 2016 Standard
- Nessus Network Monitor 5.12.0 running on Windows Server 2016 Standard
- Nessus Network Monitor 5.12.0 running on RHEL 7.7
- Log Correlation Engine 6.0.6 on RHEL 7.7
- Linux TLS Test Server.

9 TOE Evaluated Configuration

9.1 Evaluated Configuration

The TOE consists of the Nessus Manager 8.11.1 application, which is a C/C++ application with a PHP/JavaScript web front-end running on a proprietary web server. The TOE has both Linux and Windows platform versions.

The TOE is evaluated on Red Hat Enterprise Linux 7 and Windows Server 2016

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

- 4 x 2GHz cores
- 16 GB RAM
- 30 GB disk storage (direct-attached storage required).

The TOE requires the following in its operational environment:

- Other Tenable components (an instance of Tenable.sc and one or more instance of Nessus Agent applications—Nessus Network Monitor and Log Correlation Engine are expected to be present in the TOE's operational environment because they also interface with Tenable.sc but the TOE does not interact with these applications directly).
- Platform (hardware and software) on which the TOE is hosted.
  - In the evaluated configuration, RHEL 7 and Windows Server 2016 are the supported OS platforms.
- Full disk encryption is required for the TOE platform to ensure adequate data-at-rest protection.
- Web browser used to access the GUI interface.

9.2 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 the App PP or TLS Package. 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.

10 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 forTenable Nessus Manager 8.11.1 Part 2 ([11]). 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 1.3, 1 March 2019 ([5]) and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([6]). The evaluation determined the TOE satisfies the conformance claims made in the Nessus Manager 8.11.1 Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in:

- *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([5])
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([6]).

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

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

The evaluation team performed each TSS assurance 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 Protection Profile, and security function descriptions that satisfy the requirements.

10.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV assurance 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 Protection Profile 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.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance assurance 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.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance 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 Protection Profiles. 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.

10.5 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.

10.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance 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 performance of a virus scan on the installation packages for the TOE and a search of public vulnerability databases. The virus scans did not detect any virus or malware in any of the TOE installation packages.

Searches of public vulnerability repositories were performed on 4 December 2020.

The evaluation team searched the following public vulnerability repositories.

- National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search)
- SecurityFocus Database (https://www.securityfocus.com/vulnerabilities)
- US-CERT Vulnerability Notes Database (https://www.kb.cert.org/vuls/).

The evaluation team used the following search terms in the searches of these repositories:

- "tenable"
- "nessus"
- "tls v1.2"
- "openssl 1.1.1d"

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.

10.7 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 Protection Profiles. 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.

11 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 security functional requirements specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target.

Note that there is not a separate Common Criteria Configuration Guide. The information needed to use the product in the evaluated configuration, it must be configured as specified in the sub-section "Configure Tenable Nessus Manager 8.11.1 for NIAP Compliance" found within Nessus 8.11.x User Guide.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The excluded functionality is specified in section 9.2 of this report.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

12 Security Target

The ST for this product's evaluation is *Nessus Manager 8.11.1 Security Target*, Version 1.0, 4 December 2020 [7].

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
OCSP	Online Certificate Status Protocol
PCL	Product Compliant List
PII	Personally Identifiable Information
RHEL	Red Hat Enterprise Linux
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

14 Bibliography

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

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

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

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

[5] Protection Profile for Application Software, Version 1.3, 1 March 2019.

[6] Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019.

[7] Nessus Manager 8.11.1 Security Target, Version 1.0, 4 December 2020. [ST]

[8] Nessus 8.11.x User Guide, Last Revised: October 29, 2020. [User Guide]

[9] Evaluation Technical Report for Tenable Nessus Manager 8.11.1, Part 1 (Leidos Non-Proprietary), Version 1.1, 4 December 2020. [ETR P1]

[10] Evaluation Technical Report for Tenable Nessus Manager 8.11.1, Part 2 (Leidos Proprietary), Version 1.1, 4 December 2020. [ETR P2]

[11] Assurance Activities Report for Nessus Manager 8.11.1, Version 1.1, 4 December 2020. [AAR]

[12] Tenable Nessus Manager Common Criteria Test Report and Procedures, Version 1.1, 4 December 2020. [DTR]

[13] Tenable Nessus Manager Vulnerability Assessment, Version 1.1, 4 December 2020. [AVA]