National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints

Report Number: CCEVS-VR-VID10989-2019
Dated: 11 December 2019
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

Validation Team

Paul Bicknell

Sheldon Durrant

Jenn Dotson

Linda Morrison

The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Unisys Stealth Solution release v4.0 Windows and Linux Endpoints (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 Validation Report (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 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation of the Unisys Stealth Solution release v4.0 Windows and Linux Endpoints was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in December 2019.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4]) and the PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.0, 04 September 2019.

This PP-Configuration includes the following components:

- *Base-PP: Protection Profile for Application Software, Version 1.3* [5]
- *PP-Module: PP-Module for Virtual Private Network (VPN) Clients, Version 2.1* [7]

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Stealth Endpoints for Windows and Linux provide capabilities for protected transmission of private data between Stealth-enabled IPsec Virtual Private Network (VPN) endpoints. They are the components of the Unisys Stealth Solution that enables endpoint devices to establish secure IPsec tunnels with each other.

The Unisys Stealth Solution is an enterprise networking security solution that utilizes IPsec to protect the confidentiality of data transmitted between devices on the enterprise network.

The TOE comprises software installed on Windows-based servers, Windows workstations, and Linux servers. The TOE functions as an IPsec VPN client and implements a client-to-client model of operation—the Stealth Endpoints for Windows and Linux establish IPsec tunnels with each other rather than with a VPN gateway.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile (PP) and PP-Module and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST [8]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([12]) and the associated test report produced by the Leidos evaluation team ([13]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed PP and PP-Module and that the evaluation activities specified in [5] and [7] had been performed appropriately. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report (ETR) ([11]) are consistent with the evidence produced.

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).

The following table provides information needed to completely identify the product and its evaluation, 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	Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints
Security Target	Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints Security Target, Version 1.0, 3 December 2019
Sponsor & Developer	Unisys Corporation 801 Lakeview Drive Blue Bell, PA 19422
Completion Date	December 2019
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-Configuration	PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.0, 04 September 2019
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	Anthony Apted Allen Sant Kevin Steiner
Validation Personnel	Paul Bicknell Sheldon Durrant Jenn Dotson Linda Morrison

3 Architectural Information

The Windows and Linux Endpoints comprising the TOE are part of the Unisys Stealth Solution, which encompasses the following additional components, briefly discussed here to aid understanding of the TOE:

- Enterprise Manager—a management application that allows administrators to create and manage COIs, provision and monitor Stealth endpoints, and authorize, monitor, and license Stealth users. The Enterprise Manager includes the Stealth Authorization Service
- Stealth Secure Virtual Gateway—enables non-Windows and non-Linux endpoints to participate in Stealth networks
- Secure Remote Access Gateway—enables systems that are physically located outside of the enterprise's intranet to participate in an enterprise's Stealth network.

The Windows and Linux Endpoints are provisioned as endpoint installation packages that are created by the Enterprise Manager in the TOE's operational environment. The Enterprise Manager can create endpoint packages specific for Windows 10 (32-bit and 64-bit), Windows Server 64-bit platforms, and Red Hat Enterprise Linux 64-bit operating systems. The installation package includes the Stealth endpoint software and configuration information that specifies the IKE and IPsec cryptographic profiles (termed "protection profiles" in the product guidance documentation) the TOE will use when negotiating an IPsec tunnel with another endpoint. The TOE establishes the IPsec tunnel in transport mode.

The endpoints on which the package is installed validate the signature of the signing certificate using the associated trusted root certificate, which is also installed on these endpoints.

In the evaluated configuration, the Stealth Windows Endpoint is supported on Windows 10 (32-bit and 64-bit) and Windows Server 2016 (64-bit), while the Stealth Linux Endpoint is supported on Red Hat Enterprise Linux (RHEL) 7.4 (64-bit) and 7.5 (64-bit).

The physical boundary of the TOE comprises an endpoint installation package that is created by the Enterprise Manager. The installation package includes the Stealth endpoint software and configuration information that specifies the IKE and IPsec cryptographic profiles the TOE will use when negotiating an IPsec tunnel with another endpoint.

The Stealth Windows Endpoint application comprises:

- Kernel-mode drivers (`mlstpgw.sys`, `stealthii.sys`)
- The following services:
  - Unisys Stealth Logon Service (`USSL_Logon`)
  - Unisys PreLogon Service (`USSL_PreLogon`)
  - Unisys Protocol Service (`USSL_Protocol`).

The Stealth Linux Endpoint application comprises:

- `unisys-fips-libdavici-1.1.0-2`
- `unisys-libnetfilter-conntrack-1.0.5-1`
- `unisys-fips-libcurl-7.46.0-6`
- `unisys-fips-libxmlsec1-1.2.22-4`
- `unisys-fips-strongswan-5.6.3-5`

- `unisys-fips-stealth-4.0.026.0`.

All Windows endpoints on which the TOE is to be installed must have at least 2 GB of memory and must run the following software:

- .NET Framework version 3.5 with Service Pack 1, or .NET Framework version 4.x.

All Linux endpoints on which the TOE is to be installed must meet the memory and disk space requirements for the specific Linux operating system and must run the following software:

- RHEL 7.4:
  - Linux kernel 3.10.0-693.el7
  - OpenSSL 1.0.2k-8.el7
- RHEL 7.5:
  - Linux kernel 3.10.0-862.2.3.el7
  - OpenSSL 1.0.2k-8.el7.

Additionally, each endpoint on which the TOE is installed must be configured for FIPS mode.

The TOE requires the following in its operational environment:

- Management Server—a Windows Server 2012 R2 64-bit or Windows Server 2016 host, with FIPS mode configured, that runs the Enterprise Manager application, including the Stealth Authorization Service

In addition, the Management Server must be Stealth-enabled (i.e., the Stealth Windows Endpoint is installed on the Management Server as well as the VPN endpoints).

4 Security Policy

4.1 Cryptographic Support

The TOE enables an end user to establish a point-to-point VPN tunnel with another Stealth-enabled endpoint, using the underlying platform's implementation of IKE and IPsec. The Unisys Windows Stealth Endpoint invokes the platform functionality to securely store domain credentials while the Unisys Linux Stealth Endpoint does not store any domain credentials.

4.2 User Data Protection

The TOE and the TOE platforms ensure that residual information is protected from potential reuse in accessible objects such as network packets. The Stealth Windows Endpoint does not store any sensitive data in non-volatile memory. The Stealth Linux Endpoint leverages platform-provided functionality to encrypt sensitive data.

The TOE restricts network communication to user-initiated communication for Stealth-tunneled network traffic to Stealth-enabled endpoints and communication to the Stealth Authorization Service.

4.3 Identification and Authentication

The TOE provides the ability to use, store, and protect X.509v3 certificates. The TOE supports the use of X.509v3 certificates for IKE peer authentication and integrity verification. In addition, the TOE platform uses X.509v3 certificates.

4.4 Security Management

The TOE provides the following management functions:

- Specify IPsec VPN Clients to use for connections
- Specify client credentials to be used for connections
- Configure the reference identifier of the peer
- Specify IKEv2 Security Association (SA) lifetimes
- Configure packet filter rules
- Configure Certificate Revocation List (CRL) checking
- Configure algorithm suites that can be proposed and accepted during IPsec exchanges.

4.5 Privacy

The TOE does not collect or transmit Personally Identifiable Information (PII) over a network.

4.6 Protection of the TSF

The TOE relies upon its underlying platform to perform self-tests that cover the TOE as well as the functions necessary to securely update the TOE. The TOE does not allocate any memory region with both write and execute permissions and is compiled with stack-based buffer overflow protection enabled. The TOE applications use only documented platform Application Programming Interfaces (APIs).

4.7 Trusted Path/Channels

The TOE encrypts all transmitted sensitive data with IPsec between itself and another trusted IT product.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PPs to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PPs, 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.
- Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

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 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 *Supporting Document—PP-Module for Virtual Private Network (VPN) Clients*, Version 2.1, 5 October 2017 [7] and performed by the evaluation team).
- This evaluation covers only the specific software distributions and versions 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 Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints Security Target, Version 1.0, 3 December 2019 [8].
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in [8].
- 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 Validation Report.

6 Documentation

Unisys 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:

- *Unisys Stealth Solution Common Criteria Evaluation Guidance Document*, Release 4.0, October 24, 2019 (8205 5823–005) [9]
- *Unisys Stealth Information Center*, Release 4.0, April 2019 (8222 4189-013) [10].

This is also provided for initial setup purposes. To use the product in the evaluated configuration, the product must be configured as specified in these guides.

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.

7 IT Product Testing

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

- *Test Report for Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints*, Version 1.1, 21 October 2019 [13]

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

- *Assurance Activities Report for Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints*, Version 1.1, 3 December 2019 [12]

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 PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.0, 04 September 2019.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Application Software* and *Supporting Document—PP-Module for Virtual Private Network (VPN) Clients* [7]. 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.

The evaluators received the TOE in the form that normal 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* and *Supporting Document—PP-Module for Virtual Private Network (VPN) Clients* were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration comprising the following components networked together via a mirror capable switch:

- TOE components:
  - Stealth Windows Endpoint 4.0.026.0, installed on Windows Server 2016 (64 bit)
  - Stealth Windows Endpoint 4.0.026.0, installed on Windows 10 (32 bit)
  - Stealth Windows Endpoint 4.0.026.0, installed on Windows 10 (64 bit)
  - Stealth Linux Endpoint 4.0.026.0, installed on Red Hat Enterprise Linux 7.5
- Operational and test environment components:
  - Unisys Stealth Enterprise Manager, installed on Windows Server 2016, along with Stealth Windows Endpoint
  - Active Directory (AD) domain controller, installed on Windows Server 2016, with following installed features:
    - Active Directory Certificate Services

- Active Directory Domain Services
- Domain Name Service
- Internet Information Services

- Network monitor computer running Ubuntu 18.04 with Wireshark 2.6.8 and tcpdump 4.9.2—this computer was set up to monitor the traffic on the test network via the mirror capable switch and was unable to communicate directly with the TOE components
- Tester computer running Windows Server 2016 with Remote Desktop Manager version 2.7.

8 Evaluated Configuration

The TOE comprises the Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints. They are the components of the Unisys Stealth Solution that enable endpoint devices to establish secure IPsec tunnels with each other.

The physical boundary of the TOE comprises an endpoint installation package created by the Stealth Enterprise Manager. The installation package includes the Stealth endpoint software and configuration information that specifies the IKE and IPsec cryptographic profiles the TOE will use when negotiating an IPsec tunnel with another endpoint.

The evaluated configuration consists of:

- Unisys Stealth Solution Release 4.0.026.0 Windows Endpoint
- Unisys Stealth Solution Release 4.0.026.0 Linux Endpoint.

The Windows Endpoint is evaluated on:

- Windows 10 (32-bit and 64-bit)
- Windows Server 2016 (64-bit).

The Linux Endpoint is evaluated on:

- Red Hat Enterprise Linux (RHEL) 7.4 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.5 (64-bit).

All Windows endpoints on which the TOE is to be installed must have at least 2 GB of memory and must run the following software:

- .NET Framework version 3.5 with Service Pack 1 or .NET Framework version 4.x.

All Linux endpoints on which the TOE is to be installed must meet the memory and disk space requirements for the specific Linux operating system and must run the following software:

- Red Hat Enterprise Linux (RHEL) 7.4
    - Linux kernel 3.10.0-693.el7
    - OpenSSL 1.0.2k-8.el7
- Red Hat Enterprise Linux (RHEL) 7.5
    - Linux kernel 3.10.0-862.2.3.el7
    - OpenSSL 1.0.2k-12.el7.

Additionally, each endpoint on which the TOE is installed must be configured for FIPS mode.

The TOE requires the following in its operational environment:

- Management Server, which runs the services comprising the Enterprise Manager software, including the Stealth Authorization Server

In addition, the Management Server must be Stealth-enabled (i.e., the TOE is required to be installed on the Management Server as well as the VPN endpoints) and configured for FIPS mode.

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 Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints 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 PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.0, 04 September 2019 which includes the specific evaluation activities specified in *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([5]) and *Supporting Document—PP-Module for Virtual Private Network (VPN) Clients*, Version 2.1, 5 October 2017 ([7]). The evaluation determined the TOE satisfies the conformance claims made in the Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints 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])
- *PP-Module for Virtual Private Network (VPN) Clients*, Version 2.1, 5 October 2017 ([6]).

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 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 Profiles, and security function descriptions that satisfy the requirements.

9.2 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 Profiles 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 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.

9.4 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.

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

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

9.6 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 PPs. This comprised performance of a virus scan on the installation packages for the TOE, using McAfee Endpoint Security 10.6, last updated on 3 December 2019, 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 during the evaluation and then re-performed a final time on 3 December 2019 to ensure that no additional public vulnerabilities were disclosed prior to the completion of the evaluation.

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/)
- Unisys Support Product Security Vulnerability (https://public.support.unisys.com/common/public/vulnerability/NVD_Home.aspx?nav=pv).

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

- “unisys”
- “stealth”
- “vpn client”
- “ipsec”
- “ikev2”
- “strongswan”
- “rhel”
- “linux 3.10”
- “openssl”
- “windows 10”
- “windows server 2016”

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 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.

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 functionality evaluated 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. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

11 Security Target

The ST for this product's evaluation is *Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints Security Target*, Version 1.0, 3 December 2019 [8].

12 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
COI	Community of Interest
CRL	Certificate Revocation List
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IT	Information Technology
PCL	Product Compliant List
PII	Personally Identifiable Information
RHEL	Red Hat Enterprise Linux
SA	Security Association
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VPN	Virtual Private Network
VR	Validation Report
XML	Extensible Markup Language

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 1.3, 1 March 2019.

[6] PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 5 October 2017.

[7] Supporting Document—PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, October 2017.

[8] Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints Security Target, Version 1.0, 3 December 2019.

[9] Unisys Stealth Common Criteria Evaluation Guidance Document, Release 4.0, 24 October 2019.

[10] Unisys Stealth Information Center, Release 4.0, April 2019.

[11] Evaluation Technical Report for Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints, Part 2 (Leidos Proprietary), Version 1.2, 3 December 2019.

[12] Assurance Activities Report for Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints, Version 1.1, 3 December 2019.

[13] Test Report for Unisys Stealth Solution Release v4.0 Windows and Linux Endpoints, Version 1.3, 3 December 2019.