National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Unisys Stealth Solution Release v3.0 Windows Endpoint

Report Number: CCEVS-VR-VID10716-2016
Dated: July 7, 2016
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

Table of Contents

List of Tables

1 Executive Summary

This report 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. Prospective users should read carefully 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.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation Unisys Stealth Solution Release v3.0 Windows Endpoint. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Unisys Stealth Solution Release v3.0 Windows Endpoint was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in June 2016. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in the *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, with CSfC selections for VPN Clients applied. The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:

- TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0037: IPsec Requirement_DN Verification.

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 Leidos evaluation team determined that the Unisys Stealth Solution Release v3.0 Windows Endpoint is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

The TOE comprises software installed on Windows-based servers and workstations that enables these devices to participate in the Stealth network as Stealth-enabled endpoints. The TOE enables multiple "secure communities" to share the same network without fear of another group accessing their data or their workstations and servers. These are referred to as Communities of Interest (COIs). The TOE functions as an IPsec VPN client that enables the endpoint on which it is installed to establish an IPsec tunnel with another Stealth-enabled endpoint belonging to the same Stealth COI. Note that the TOE implements a client-to-client model of operation—Stealth-enabled endpoints establish IPsec tunnels with each other rather than with a VPN gateway. The Windows-based servers and workstations are considered part of the operational environment.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

Table 1: Evaluation Details

Item	**Identifier**
Evaluated Product	Unisys Stealth Solution Release v3.0 Windows Endpoint
Sponsor & Developer	Unisys Corporation 801 Lakeview Drive Blue Bell, PA 19422 United States
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	June 2016
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, with CSfC selections for VPN Clients applied. The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation: • TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4 • TD0037: IPsec Requirement_DN Verification
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the Unisys Stealth Solution Release v3.0 Windows Endpoint.
Evaluation Personnel	Dawn Campbell Kevin Steiner Cody Cummins
Validation Personnel	Paul Bicknell, Dr. Patrick Mallet, Lisa Mitchell, and The MITRE Corporation

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) 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 information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Unisys Stealth Solution Release v3.0 Windows Endpoint Security Target
ST Version	1.0
Publication Date	June 16, 2016
Vendor	Unisys Corporation
ST Author	Leidos
TOE Reference	Unisys Stealth Solution Release v3.0 Windows Endpoint
TOE Software Version	Unisys Stealth Solution Release v3.0 Windows Endpoint
Keywords	IPsec VPN endpoint, VPN Client

2.1 Threats

The ST references the *Protection Profile for IPsec Virtual Private Network (VPN) Clients* to identify the following threats that the TOE and its operational environment are intended to counter:

- Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is done being used.

2.2 Organizational Security Policies

The *Protection Profile for IPsec Virtual Private Network (VPN) Clients* does not identify any organizational security policies.

3 Architectural Information

The TOE is the Unisys Stealth™ Solution Release 3.0 Windows Endpoint and it provides capabilities for protected transmission of private data between Stealth-enabled IPsec VPN endpoints.

The TOE comprises an endpoint installation package that is created by the Enterprise Manager software in the TOE's operational environment. The Enterprise Manager can create endpoint packages specific for both 32-bit and 64-bit Windows platforms. The installation package includes the Stealth endpoint software and configuration information that specifies the IKE and IPsec cryptographic profiles[1] the TOE will use when negotiating an IPsec tunnel with another endpoint.

The configuration information is contained in two XML files—"protectionprofile.xml" and "crypto.xml". The protectionprofile.xml file contains the settings the administrator configures to enable Stealth to conform to the Protection Profile for IPsec VPN Clients.

The protectionprofile.xml file is used in the process of creating endpoint packages. During the endpoint package generation process, the Enterprise Manager reads the protectionprofile.xml file, validates it, and inserts the contents into the crypto.xml file. Enterprise Manager signs the resulting crypto.xml file using a signing certificate and includes it in the endpoint package. The resulting endpoint package is then installed on the endpoints.

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

After the signing certificate has been validated, the Secure Community of Interest Protocol (SCIP) is used to attempt to establish a tunnel using the information in the crypto.xml file.

Endpoints are able to communicate using the first matching protection profile that they share. (Endpoints might be running Stealth endpoint software created with identical protectionprofile.xml profile priority lists, or they might have been created using a different profile priority list.) The profile that is used during Stealth tunnel establishment depends on the profile priority list specified on the endpoint receiving the Stealth tunnel request.

[1] These are termed "protection profiles" in the TOE guidance documentation.

4 Assumptions

The ST references the *Protection Profile for IPsec Virtual Private Network (VPN) Clients* to identify following assumptions about the use of the product:

- 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.

4.1 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
   a. Non-FIPS mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
6. During the evaluation questions were raised about testing in FCS_IPSEC_EXT.1.1 required by pp_vpn_ipsec_client_v1.4. Since the release of that PP, clarifications to similar testing in other PPs (i.e., the NDcPP v1.0) have been made. NIAP agreed that the clarified tests were to be used in this evaluation.
7. The TOE is supported on the following platforms in its operational environment that have all completed Common Criteria evaluations under the US Common Criteria Evaluation and Validation Scheme (CCEVS)—the relevant Validation Identifiers (VIDs) are provided:
   - Windows 8 (VID #10520)
   - Windows 8.1 (VID #10592)
   - Windows Server 2012 R2 (VID #10529).

   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
- Java 7.x or later (Java Runtime Platform 1.7 or later)

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

The TOE requires the following in its operational environment:

- A Management Server, which runs the services comprising the Enterprise Manager component
- The Management Server and all endpoints must be part of an Active Directory (AD) domain.

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). However, unlike the endpoints on which the TOE is installed, the Management Server must not be configured for FIPS mode.

During evaluation testing, the TOE was tested on the following specific platforms:

- Windows 8 Pro 64-bit (Version 6.2.9200)
- Windows 8.1 Pro 32-bit (Version 6.3.9600)
- Windows Server Standard 2012 R2 64-bit (Version 6.3.9600).

For the purposes of testing, these platforms were installed on a Dell PowerEdge 1950 with:

- Intel Xeon E5430 (2.66 GHz, 64-bit, 12 MB L2 Cache)
- 2GB DDR2 SDRAM
- VMware ESXi 6.0.0.

5 Security Policy

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

5.1 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.

5.2 User Data Protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

5.3 Identification and Authentication

The TOE supports the use of X.509v3 certificates for IKE peer authentication. The TOE platform provides the ability to use, store, and protect these X.509v3 certificates and performs certificate validation.

5.4 Security Management

The TOE provides capabilities necessary to manage most of its security functionality. The TOE platform implements the security management functions not provided by the TOE.

5.5 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.

5.6 Trusted Path/Channels

The TOE acts as a VPN client using IPsec to establish point-to-point secure channels with corresponding VPN clients.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, there are four Common Criteria specific guides that reference the security-related guidance material for all products evaluated:

- *Unisys Stealth Solution Common Criteria Evaluation Guidance Document*, Release 3.0, June 2016 (8205 5823–000)
- *Unisys Stealth Solution Information Center*, Release 3.0, May 2016 (8222 4189-003)
- *Unisys Stealth Solution Quick Start Implementation Guide*, Release 3.0, September 2015 (8231 0822-001).
- *Unisys Stealth Solution Release Notes*, Release 3.0, June 2016 (8230 6713-028).

Supporting TOE Guidance Documentation

- *Unisys Stealth Solution Release v3.0 Windows Endpoint Security Target*, v1.0, June 16, 2016

7 Independent Testing

This section describes the testing efforts of the evaluation team.

The purpose of this activity was to confirm the TOE behaved in accordance with the TOE security functional requirements as specified in the ST, with CSfC selections for VPN Clients applied.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, and the following NIAP Technical Decisions:

- TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0037: IPsec Requirement_DN Verification

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.

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.

The following hardware and software components were included in the evaluated configuration during testing:

- TOE Software
    - Unisys Stealth Solution Release v3.0 Windows Endpoint
- TOE Platforms
    - Each TOE OS platform was installed as a virtual machine on VMware ESXi 6.0.0
        - Windows 8 Pro 64-bit: 6.3.9600
        - Windows 8.1 Pro 32-bit: 6.2.9200
        - Windows Server Standard 2012 R2 64-bit: 6.3.9600.
- TOE Hardware platform
    - Each TOE platform was installed on a Dell PowerEdge 1950 with:
        - Intel Xeon E5430
            - 2.66 GHz
            - 64-bit
            - 12 MB L2 Cache
        - 2GB DDR2 SDRAM
- Test Environment Components
    - Certificate Authority server
    - Enterprise Manager
    - CDP
    - Test Client w/ Network Packet Monitor

The configuration proposed for testing of the TOE matched that which was defined in the Security Target.

The evaluated version of the TOE was installed and configured according to the *Unisys Stealth Solution Common Criteria Evaluation Guidance Document,* Release 3.0, March 2016 (8205 5823–000).

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, and the NIAP Technical Decisions listed above, were satisfactorily fulfilled.

7.1 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration.

8 Results of the Evaluation

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013, with CSfC selections for VPN Clients applied. The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:

- TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0037: IPsec Requirement_DN Verification.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

Regarding item number 6 in Section 4.1 (Clarifications of Scope), the Validators agreed with the use of the clarified test requirements.

The validators have no further comments about the evaluation results.

10 Annexes

Not applicable

11 Security Target

- Unisys Stealth Solution Release v3.0 Windows Endpoint Security Target, v1.0, June 16, 2016

12 Abbreviations and Acronyms

Abbreviation	Description
CC	Common Criteria
CDP	CRL Distribution Point
COI	Community of Interest
PP	Protection Profile
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function(s)

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Unisys Stealth Solution Release v3.0 Windows Endpoint Security Target, v1.0, June 16, 2016

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report For Unisys Stealth Solution Release v3.0 Windows Endpoint, Part 2 (Leidos Proprietary), Version 1.0, 16 June 2016