National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Microsoft Windows 10 IPsec VPN Client

Report Number: CCEVS-VR-10746-2016
Dated: November 10, 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

ACKNOWLEDGEMENTS

Validation Team

Meredith Hennan,
Kenneth Stutterheim,
The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos
Columbia, MD

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 to determine 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) as well as this Validation Report (VR) (which describes how those security claims were evaluated, tested, and any restrictions that may be imposed upon the evaluated configuration) to help in that determination. 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.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Microsoft Windows 10 IPsec VPN Client. 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 Microsoft Windows 10 IPsec VPN Client was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in November 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 the assurance activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4 and any applicable NIAP Technical Decisions for the technology. 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 Microsoft Windows 10 IPsec VPN Client is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfied all of the security functional requirements stated in the ST. The information in this VR is largely derived from the publically available Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The TOE is a software solution that consists of Microsoft Windows 10 Operating System editions:

- Microsoft Windows 10 Enterprise (64-bit version)
- Microsoft Windows 10 Pro (64-bit version)

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 PP had been completed successfully and that the product satisfied all of the security functional and assurance requirements as 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.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Microsoft Windows 10 IPsec VPN Client Security Target (ST).

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Microsoft Windows 10 Enterprise and Windows 10 Pro, 64-bit, with Surface Book and Surface Pro 4
Sponsor & Developer	Michael Grimm Microsoft Corporation
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	November 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
Disclaimer	The information contained in this Validation Report is not an endorsement of the Microsoft Windows 10 IPsec VPN Client by any agency of the U.S. Government and no warranty of the Microsoft Windows 10 IPsec VPN Client is either expressed or implied.
Evaluation Personnel	Gregory Beaver Gary Grainger Kevin Steiner
Validation Personnel	Meredith Hennan Kenneth Stutterheim

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	Microsoft Windows 10 IPsec VPN Client Security Target
ST Version	0.07
Publication Date	October 28, 2016
Vendor and ST Author	Microsoft
TOE Reference	Microsoft Windows 10
TOE Software Version	Microsoft Windows 10 64-bit Pro edition Microsoft Windows 10 64-bit Enterprise edition With all critical updates as of May 30, 2016
Keywords	IPsec VPN Client

2.1 Threats

The ST identifies 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

There are no Organizational Security Policies for the IPsec VPN Client protection profile.

3 Architectural Information

The TOE is a software solution that consists of Microsoft Windows 10 Operating System 64-bit Pro and Enterprise editions and those applications necessary to manage, support, and configure the operating system in order to provide IPsec VPN client capabilities. The TOE was tested on the following devices:

- Microsoft Surface Book
- Microsoft Surface Pro 4

Windows 10 is a preemptive multitasking, multiprocessor, and multi-user operating system. In general, operating systems provide users with a convenient interface to manage underlying hardware. They control the allocation of, and manage computing resources such as processors, memory, and Input/Output (I/O) devices. Windows expands these basic operating system capabilities to controlling the allocation and managing higher level IT resources such as security principals (user or machine accounts), files, printing objects, services, window station, desktops, cryptographic keys, network ports traffic, directory objects, and web content. Multi-user operating systems such as Windows keep track of which user is using which resource, grant resource requests, account for resource usage, and mediate conflicting requests from different programs and users.

The TOE includes the following variants of Windows:

- Windows 10 64-bit Pro
- Windows 10 64-bit Enterprise

The TOE operational environment included Surface Book and Surface Pro 4 hardware platforms in a networked environment with IEEE 802.11 (Wi-Fi). The following administrator, user, and configuration guides were evaluated as part of the TOE:

- *Microsoft Windows Common Criteria Evaluation Windows 10 IPsec VPN Client Operational Guidance* along with all the documents referenced therein.

4 Assumptions

The ST identifies the 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 clarification. 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 operating system editions, and software versions 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 PP and any relevant NIAP Technical Decisions. Any additional security related functional capabilities of the product were not covered by this evaluation. Any additional non-security related functional capabilities of the product, even those described in the ST, were not covered by this evaluation.
4. Per the Operational Guidance, many configurations described for the IT Administrator role are applied to the device through a Mobile Device Management (MDM) solution. The specific steps to perform a configuration through the MDM are solution-specific and are not described nor can any claims be made as to their effectiveness or correct operation. As such, examples of possible configuration option text are provided but not guaranteed to match any specific MDM solution. No MDMs were evaluated as part of the IPSec VPN client evaluation.
5. 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 Security Policy

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

5.1 Security Audit

Windows has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes the date and time of the event, the user identity that caused the event to be generated, and other event specific data. Authorized administrators can review audit logs and have the ability to search and sort audit records. Authorized Administrators can also configure the audit system to include or exclude potentially auditable events to be audited based on a wide range of characteristics. In the context of this evaluation, the protection profile requirements cover generating audit events and selecting which events should be audited.

5.2 Cryptographic Support

Windows provides FIPS validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement (which is not studied in this evaluation), and random number generation. The TOE additionally provides support for public keys, credential management and certificate validation functions and provides support for the National Security Agency's Suite B cryptographic algorithms. Windows also provides extensive auditing support of cryptographic operations, the ability to replace cryptographic functions and random number generators with alternative implementations, and a key isolation service designed to limit the potential exposure of secret and private keys. In addition to using cryptography for its own security functions, Windows offers access to the cryptographic support functions for user-mode and kernel-mode programs. Public key certificates generated and used by Windows authenticate users and machines as well as protect both user and system data in transit.

IPsec: Windows implements IPsec to provide protected, authenticated, confidential, and tamper-proof networking between two peer computers.

5.3 User Data Protection

In the context of this evaluation Windows protects user data by means of protected network tunnel based on IPsec and zeroizes memory before it is allocated to a subject process.

5.4 Identification and Authentication

In the context of this evaluation, Windows provides the ability to use, store, and protect X.509 certificates that are used for IPsec VPN sessions along with capability to use a pre-shared key.

5.5 Protection of the TOE Security Functions

Windows provides a number of features to ensure the protection of TOE security functions. Windows protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols including IPsec, IKE, and ISAKMP. Windows ensures process isolation security for all processes through private virtual address spaces, execution context, and security context. The Windows data structures defining process address space, execution context, memory protection, and security context are stored in protected kernel-mode memory. Windows includes self-testing features that ensure the integrity of executable program images and its cryptographic functions. Finally, Windows provides a trusted update mechanism to update Windows binaries itself.

5.6 Trusted Path for Communication

Windows uses the IPsec suite of protocols to provide a Virtual Private Network Connection (VPN) between itself, acting as a VPN client, and a VPN gateway.

5.7 Security Management

Windows includes several functions to manage security policies. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

6 Documentation

Microsoft offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Microsoft Windows 10 IPsec VPN Client Operational Guidance, Version 1.0, October 12, 2016.

The above document is considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

The Security Target used is:

- Microsoft Windows 10 IPsec VPN Client Security Target, Version 0.07, October 28, 2016

7 Independent Testing

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

- *Windows 10 VPN Client Common Criteria Test Report and Procedures,* Version 0.3, July 20, 2016

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- *Microsoft Windows 10 IPsec VPN Client Common Criteria Assurance Activities Report*, Version 1.2, October 28, 2016

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 claiming conformance to *Protection Profile for IPsec Virtual Private Network (VPN) Clients,* version 1.4.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for IPsec Virtual Private Network (VPN) Clients,* version 1.4. 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 primarily at the Leidos CCTL location in Columbia, Maryland. The evaluation team performed limited testing at Microsoft facilities in Redmond, Washington.

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 IPsec Virtual Private Network (VPN) Clients,* version 1.4, were fulfilled.

8 Evaluated Configuration

The evaluated version of the TOE consists of the following software.

TOE Software Identification: The following Windows Operating System editions are included in the evaluation:

- Microsoft Windows 10 Pro (64-bit version)
- Microsoft Windows 10 Enterprise (64-bit version)

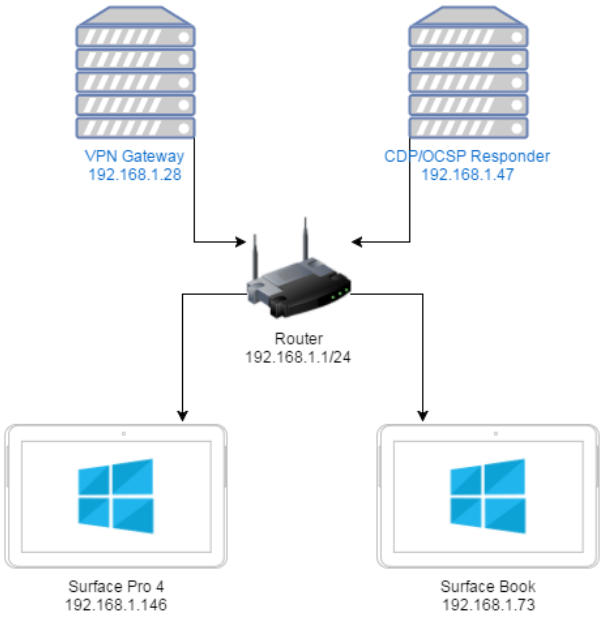
The following security updates must be applied to the above Windows 10 products:

- All critical updates as of May 30, 2016

The TOE must be deployed as described in section 4 Assumptions of this document and be configured in accordance with the *Microsoft Windows 10 IPsec VPN Client Operational Guidance*, Version 1.0, October 12, 2016. Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

The TOE operational environment used during evaluation included the Surface Book and Surface Pro 4 hardware platforms in a networked environment with IEEE 802.11 (Wi-Fi).



9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for IPsec Virtual Private Network (VPN) Clients Version 1.4, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

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 function 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 – sample
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by Microsoft Windows 10 IPsec VPN Client, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Those employing the Windows 10 IPsec VPN Client must follow the configuration instructions provided in the Operational guidance documentation listed above to ensure the evaluated configuration is established and maintained. Note that operation in FIPS validated mode is required.

The validators encourage the consumers of these products to understand the relationship between the products and any functionality that may be provided via Mobile Device Management solutions. This evaluation does not cover, nor does it endorse the use of any particular MDM solution and only the MDM interfaces of the products were exercised as part of the evaluation.

Consumers should be aware that the full extent of vulnerability analysis exercised against the product was limited to a series of search terms levied against the National Vulnerability Database for public vulnerability information in the form of Common Vulnerabilities and Exposures (CVEs).

Astute readers of the Security Target for this product may notice that the ST includes information regarding CSfC requirements. These are included as a courtesy to those consumers who require CSfC approvals.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	Microsoft Windows 10 IPsec VPN Client Security Target
ST Version	0.07
Publication Date	October 28, 2016

13 Abbreviations and Acronyms

AGD	Administrator Guidance Document
CC	Common Criteria
CM	Configuration Management; Control Management
CSfC	Commercial Solutions for Classified Program
FIPS	Federal Information Processing Standard
GPOSPP	U.S. Government Approved Protection Profile - Protection Profile for General Purpose Operating Systems
I/O	Input / Output
ID	Identification
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
US	United States
VPN	Virtual Private Network

14 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] *Microsoft Windows 10 IPsec VPN Client Security Target,* Version 0.07, October 28, 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 Microsoft Windows 10 IPsec VPN Client,* Version 1.1, October 28, 2016

[8] *Microsoft Windows 10 IPsec VPN Client Operational Guidance,* Version 1.0, October 12, 2016