National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Protection Profile for General Purpose Operating Systems, Version 4.2.1, 22 April 2019

Report Number:	**CCEVS-VR-PP-0047**
Dated:	**01 May 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

Common Criteria Testing Laboratory

Base and Additional Requirements

Epoche and Espri S.L.U
Av. de los Pirineos, 7, Nave 9A
28703 San Sebastián de los Reyes
Madrid, Spain

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for General Purpose Operating Systems, Version 4.2.1, 22 April 2019 (GPOS PP v4.2.1). It presents a summary of the GPOS PP v4.2.1 and the evaluation results.

The initial evaluation of the General Purpose Operating Systems, Version 4.2, 22 May 2018 (GPOS PP v4.2) was performed concurrently with the first product evaluation. The Target of Evaluation (TOE) was Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update), evaluated by Epoche & Espri S.L.U in Madrid, Spain.

This evaluation addressed the base requirements of the GPOS PP v4.2. The PP also includes several optional, selection-based, and objective requirements. The TOE claimed some but not all of these requirements. Requirements that were not claimed by the TOE were evaluated separately as part of the completion of the APE assurance requirements of the Common Criteria.

The Validation Report (VR) author independently performed an additional review of the GPOS PP v4.2 as part of the development of this VR, to confirm it met the claimed APE assurance requirements.

The evaluation determined the GPOS PP v4.2 was both Common Criteria Part 2 Extended and Part 3 Extended. An accredited CCTL evaluated the GPOS PP v4.2 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), as well as additional scheme guidance required by NIAP. The Security Target (ST) included material from both the PP_OS_v4.2 and an Extended Package (EP). Only the portions of the ST evaluation that related to the PP_OS_v4.2 were considered for the VR; the EP materials were not considered.

The initial results by the validation team found that the evaluation showed that the GPOS PP v4.2 did not meet the requirements of the APE components. The majority of the findings were typographical errors related to the conventions for indicating assignments and selections and some SFR mappings to objectives and their rationale were missing. These findings were confirmed by the VR author and NIAP. NIAP determined the impact of the changes were minor and did not affect the security functionality of the PP. Subsequently, NIAP corrected all deficiencies, and published a minor revision, GPOS PP v4.2.1. As a result, the validation team confirmed that the GPOS PP v4.2.1 meets the requirements of the APE components.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

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 CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and EPs that have Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP or EP.

The evaluation of the GPOS PP v4.2.1 was performed concurrent with the first product evaluation against the PP requirements. In this case the Target of Evaluation (TOE) was Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update), performed by Epoche & Espri S.L.U in Madrid, Spain.

The GPOS PP v4.2.1 has a set of "base" requirements all conformant STs must include and also has "Optional," "Selection-based," and "Objective" requirements. Optional requirements define functionality subjected to security evaluation that not all conformant TOEs need to include. Selection-based requirements must be included based on the selections made in the base requirements and the capabilities of the TOE. Objective requirements are those the PP sponsor intends to mandate in future versions, and are included as optional requirements that raise industry awareness of expected future requirements. This evaluation claimed some of the functions identified in these requirements.

A specific ST may not include these discretionary requirements, so the initial use of the PP addresses (in terms of the PP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ work units performed against the GPOS PP v4.2.1. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the GPOS PP v4.2.1 were evaluated.

The following identifies the GPOS PP v4.2.1 that was evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this PP and any subsequent evaluations that address additional optional, selection-based, or objective requirements in the PP.

Protection Profile	Protection Profile for General Purpose Operating Systems, Version 4.21, 22 April 2019
ST (Base)	Microsoft Windows 10 version 1809 (October 2018 Update) and Microsoft Windows Server 2019 version 1809 (October 2018 Update) Security Target version 0.03, February 21, 2019
Assurance Activity Report (Base)	MS-W10-1809-ASE; Microsoft Windows Common Criteria Evaluation Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update) ASE Partial Report, 22-02-2019, Version 2.0
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Epoche & Espri S.L.U Avenida de los Pirineos, 7 Nave 9A 28703, San Sebastián de los Reyes (Madrid, Spain)

3 GPOS PP v4.2.1 Description

The GPOS PP v4.2.1 specifies information security requirements for operating systems, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

An operating system in the context of this PP is software that manages computer hardware and software resources, and provides common services for application programs. The hardware it manages may be physical or virtual.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections should exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
A.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

4.2 Threats

The following table shows the applicable threats from GPOS PP v4.2.1.

Table 2: Threats

Threat Name	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.

T.LOCAL_ATTACK	An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.
T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

4.3 Organizational Security Policies

The following table shows applicable organizational security policies from GPOS PP v4.2.1.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
This PP does not define any organizational security policies.	

4.4 Security Objectives

The following table shows security objectives for the TOE from GPOS PP v4.2.1.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.ACCOUNTABILITY	Conformant OSes ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.
O.INTEGRITY	Conformant OSes ensure the integrity of their update packages. OSes are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant OSes provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant OSes provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration and application execution control.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant OSes provide data-at-rest protection for credentials. Conformant OSes also provide access controls which allow users to keep their files private from other users of the same system.

Requirement Class	ST Requirement Component	PP Requirement Component	Verified By
			1809 (October 2018 Update)
	FCS_COP.1(SYM) Cryptographic Operation for Data Encryption/Decryption	FCS_COP.1(1) Cryptographic Operation - Encryption/Decryption (Refined)	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FCS_COP.1(HASH) Cryptographic Operation for Hashing	FCS_COP.1(2) Cryptographic Operation - Hashing (Refined)	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FCS_COP.1(SIGN) Cryptographic Operation for Signing	FCS_COP.1(3) Cryptographic Operation - Signing (Refined)	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FCS_COP.1(HMAC) Cryptographic Operation for Keyed Hash Algorithms	FCS_COP.1(4) Cryptographic Operation - Keyed-Hash Message Authentication (Refined)	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FCS_RBG_EXT.1 Random Bit Generation	FCS_RBG_EXT.1 Random Bit Generation	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FCS_STO_EXT.1 Storage of Sensitive Data	FCS_STO_EXT.1 Storage of Sensitive Data	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FCS_TLSC_EXT.1 TLS Client Protocol	FCS_TLSC_EXT.1 TLS Client Protocol	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update
FDP: User Data Protection	FDP_ACF_EXT.1 Access Controls for Protecting User Data	FDP_ACF_EXT.1 Access Controls for Protecting User Data	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
FMT: Security Management	FMT_MOF_EXT.1 Management of security functions behavior	FMT_MOF_EXT.1 Management of security functions behavior	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)

Requirement Class	ST Requirement Component	PP Requirement Component	Verified By
	FMT_SMF_EXT.1 Specification of Management Functions	FMT_SMF_EXT.1 Specification of Management Functions	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
FPT: Protection of the TSF	FPT_ACF_EXT.1 Access controls	FPT_ACF_EXT.1 Access controls	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FPT_ASLR_EXT.1 Address Space Layout Randomization	FPT_ASLR_EXT.1 Address Space Layout Randomization	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FPT_SBOP_EXT.1 Stack Buffer Overflow Protection	FPT_SBOP_EXT.1 Stack Buffer Overflow Protection	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FPT_TST_EXT.1 Boot Integrity	FPT_TST_EXT.1 Boot Integrity	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FPT_TUD_EXT.1 Trusted Update	FPT_TUD_EXT.1 Trusted Update	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FPT_TUD_EXT.2 Trusted Update for Application Software	FPT_TUD_EXT.2 Trusted Update for Application Software	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
FAU: Audit Data Generation	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 Audit Data Generation (Refined)	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
FIA: Identification and Authentication	FIA_AFL.1 Authentication failure handling	FIA_AFL.1 Authentication failure handling (Refined)	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FIA_UAU.5 Multiple Authentication Mechanisms	FIA_UAU.5 Multiple Authentication Mechanisms (Refined)	Microsoft Windows 10 and Windows Server 2019 version

Requirement Class	ST Requirement Component	PP Requirement Component	Verified By
			1809 (October 2018 Update)
	FIA_X509_EXT.1 X.509 Certificate Validation	FIA_X509_EXT.1 X.509 Certificate Validation	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FIA_X509_EXT.2 X.509 Certificate Authentication	FIA_X509_EXT.2 X.509 Certificate Authentication	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
FTP: Trusted Path/Channels	FTP_ITC_EXT.1(TLS) Trusted Channel Communication	FTP_ITC_EXT.1 Trusted channel communication	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FTP_ITC_EXT.1(DTLS) Trusted Channel Communication	FTP_ITC_EXT.1 Trusted channel communication	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FTP_TRP.1 Trusted Path	FTP_TRP.1 Trusted Path	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)

The following table shows the "**Optional**" requirements included in Appendix A, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

Table 7: Optional Requirements

Requirement Class	ST Requirement Component	PP Requirement Component	Verified By
FCS: Cryptographic Support	FCS_TLSC_EXT.4 TLS Client Protocol	FCS_TLSC_EXT.4 TLS Client Protocol	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
FDP: User Data Protection	FDP_IFC_EXT.1 Information flow control	FDP_IFC_EXT.1 Information flow control	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)

FTA: TOE Access	FTA_TAB.1 Default TOE access banners	FTA_TAB.1 Default TOE access banners	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)

The following table shows the "**Selection-Based**" requirements included in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). These requirements are found in an ST if the ST authors make associated selections in requirements levied on the TOE by the ST.

Table 8: Selection-Based Requirements

Requirement Class	ST Requirement Component	PP Requirement Component	Verified By
FCS: Cryptographic Support	FCS_TLSC_EXT.2 TLS Client Protocol	FCS_TLSC_EXT.2 TLS Client Protocol	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	FCS_DTLS_EXT.1 DTLS Implementation	FCS_DTLS_EXT.1 DTLS Implementation	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)

The following table shows the "**Objective**" requirements included in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

Table 9: Objective Requirements

Requirement Class	ST Requirement Component	PP Requirement Component	Verified By
FCS: Cryptographic Support	FCS_TLSC_EXT.3 TLS Client Protocol	FCS_TLSC_EXT.3 TLS Client Protocol	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
FPT: Protection of the TSF	FPT_SRP_EXT.1 Software Restriction Policies	FPT_SRP_EXT.1 Software Restriction Policies	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	N/A	FPT_W^X_EXT.1 Write XOR Execute Memory Pages	PP Evaluation

6 Assurance Requirements

The following shows the assurance requirements included in the GPOS PP v4.2.1.

Table 10: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	ASE_ECD.1: Extended Components Definition	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	ASE_INT.1: ST Introduction	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	ASE_OBJ.1: Security Objectives for the Operational Environment	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	ASE_REQ.1: Stated Security Requirements	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	ASE_SPD.1: Security Problem Definition	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	ASE_TSS.1: TOE Summary Specification	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
ADV: Development	ADV_FSP.1 Basic Functional Specification	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	AGD_PRE.1: Preparative Procedures	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	ALC_CMS.1: TOE CM Coverage	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
	ALC_TSU_EXT.1: Timely Security Updates	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
ATE: Tests	ATE_IND.1: Independent Testing - Conformance	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)

Requirement Class	Requirement Component	Verified By
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)

7 Results of the Evaluation

Note that for APE elements and work units identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 11: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
APE_ECD.1	Pass	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
APE_INT.1	Pass	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
APE_OBJ.1	Pass	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
APE_REQ.1	Pass	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)
APE_SPD.1	Pass	Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update)

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the GPOS PP v4.2 Assurance Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process the CCEVS Validation Body uses that leads to the issuance of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 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, dated: April 2017.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: 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, dated: April 2017.

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

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Protection Profile for General Purpose Operating Systems, Version 4.2, 22 May 2018

[7] Protection Profile for General Purpose Operating Systems, Version 4.2.1, 22 April 2019

[8] Microsoft Windows 10 version 1809 (October 2018 Update) and Microsoft Windows Server 2019 version 1809 (October 2018 Update) Security Target version 0.03, February 21, 2019

[9] MS-W10-1809-ASE Version 2.0, Microsoft Windows Common Criteria Evaluation Microsoft Windows 10 and Windows Server 2019 version 1809 (October 2018 Update) ASE Partial Report, February 22, 2019