National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Microsoft Windows 8, Microsoft Windows Server 2012 General Purpose Operating System

Report Number: CCEVS-VR-VID10520-2015
Dated: 09 January 2015
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

Members from

The Aerospace Corporation,
The Mitre Corporation,
National Security Agency

Common Criteria Testing Laboratory

Leidos (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Microsoft Windows 8 (Pro and Enterprise Editions) and Microsoft Windows Server 2012 (Standard and Datacenter Editions) General Purpose Operating Systems (GPOS) products was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in December 2014. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 (as documented in Part 2 of the General-Purpose Operating System Protection Profile, version 3.9 (GPOSPP)) and assurance activities specified in the GPOSPP. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The GPOSPP was developed jointly by NIAP and Bundesamt für Sicherheit in der Informationstechnik (BSI), and this evaluation was conducted as a trial for the document. The published GPOSPP was supplemented by assurance activities and functional requirements (primarily concerning cryptographic functionality) agreed to by NIAP, the CCTL, and the vendor, and are captured in the ST. Where the existing GPOSPP requirements or assurance activities required modification or elaboration due to the trial nature of the evaluation, activities were defined, agreed to, and performed by the CCTL with oversight from the validation team. These activities were consistent with Part 2 of the GPOSPP as well as the work units defined in the CEM. These issues and resolutions are documented in a proprietary issue resolution report.

The Leidos evaluation team determined that the product is conformant to the GPOSPP. The information in this Validation Report is largely derived from the *Microsoft Windows 8, Windows RT, Server 2012 Operating System Assurance Activity Report, v0.7, December 15th, 2014* (AAR) (which contains information typically found in an Evaluation Technical Report (ETR)), Evaluation Technical Report (ETR) sections for activities not covered by the AAR, technical discussions with the evaluation team, and test reports produced by the Leidos evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

Windows 8 editions included in the evaluated configuration are suited for business desktops and notebook computers. Each edition is a workstation product and while it can be used by itself, it is designed to serve as a client within Windows domains.

Built for workloads ranging from the department to the enterprise to the cloud, Windows Server 2012 Standard and Datacenter editions deliver intelligent file and printer sharing; secure connectivity based on Internet technologies, and centralized desktop policy management. It provides the necessary scalable and reliable foundation to support mission-critical solutions for databases, enterprise resource planning software, high-volume, real-time transaction processing, server consolidation, public key infrastructure, and additional server roles.

Windows 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 and manage computing resources such as processors, memory, and Input/Output (I/O) devices. Windows 8 and Windows Server 2012, collectively referred to as Windows, expand 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.

In terms of security, Windows product variants share the same security characteristics. The primary difference is that the Server 2012 products include services and capabilities that are not part of other Windows editions (for example the DNS Server, DHCP Server) or are not installed by default on Server 2012 (for example the Windows Media Player, Windows Aero and desktop themes). The additional services have a bearing on the security properties of the distributed operating system (e.g., by extending the set of available interfaces and proffered services) and as such are included within the scope of the evaluation. The specific differences between the different editions of Windows are described in the TOE summary specification of the *Microsoft Windows 8, Microsoft Windows Server 2012 Security Target* (ST).

Windows provides an interactive User Interface (UI), as well as a network interface. The TOE includes a set of Windows 8 and Server 2012 systems that can be connected via their network interfaces and organized into domains and forests. A domain is a logical collection of Windows systems that allows the administration and application of a common security policy and the use of a common accounts database. One or more domains combine to comprise a forest. Windows supports single-domain and multiple-domain (i.e., forest) configurations as well as federation between forests and external authentication services.

Each domain must include at least one designated server known as a Domain Controller (DC) to manage the domain. The TOE allows for multiple DCs that replicate TOE user and machine account as well as group policy management data among themselves to provide for higher availability.

Each Windows system, whether it is a DC server, non-DC server, or workstation, provides a subset of the TSFs. The TSF subset for Windows 8 and Windows Server 2012 can consist of the security functions from a single system, for a stand-alone system, or the collection of security functions from an entire network of systems, for a domain configuration.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the ST.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Windows 8 (Pro and Enterprise Editions), Windows Server 2012 (Standard and Datacenter Editions)
Sponsor:	Microsoft Corporation
Developer:	Microsoft Corporation
CCTL:	Leidos (formerly SAIC) 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	05 February 2013
Completion Date:	09 January 2015
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 4, September 2012.
Evaluation Class:	Operating System
Description:	The TOE is a general-purpose, distributed, network operating system that provides controlled access between subjects and user data objects.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Microsoft Windows 8, Microsoft Windows Server 2012 Operating System product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	General-Purpose Operating System Protection Profile, Version 3.9, 15 January 2013
Evaluation Personnel:	Leidos (formerly SAIC): *Gary Grainger* *Anthony Apted* *Gregory Beaver* *Dawn Campbell* *Kevin Steiner* *Haley Johnson*
Validation Body:	National Information Assurance Partnership, CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- A threat agent may read or modify TSF data using functions of the TOE without the necessary authorization.
- A threat agent may gain access to user data stored, processed or transmitted by the TOE without being appropriately authorized according to the TOE security policy by using functions provided by the TOE.

- A threat agent may access cryptographically protected data transferred via a trusted channel between the TOE and another remote trusted IT system, modify such data during transfer in a way not detectable by the receiving party or masquerade as a remote trusted IT system.
- A threat agent may send data packets to the recipient in the TOE via a network communication channel in violation of the information flow control policy.
- A threat agent may masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to user data, TSF data, or TOE resources.
- A threat agent may gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated by the TSF.
- A threat agent may gain unauthorized access to an unattended session.
- A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.

1.4 Organizational Security Policies

The ST identifies the following Organizational Security Policies that the TOE and its operational environment implement:

- The users of the TOE shall be held accountable for their security-relevant actions within the TOE.
- Authority shall only be given to users who are trusted to perform the actions correctly.
- The TOE shall use standards-based cryptography as a baseline for key management (i.e., generation and destruction) and for cryptographic operations (i.e., encryption, decryption, signature, hashing, and random number generation).
- Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has.

2 Identification

The evaluated product is **Microsoft Windows 8 and Microsoft Windows Server 2012**, covering the Pro and Enterprise Editions of Windows 8, and the Standard and Datacenter Editions of Windows Server 2012.

3 Security Policy

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

> ***Note:*** *Much of the description of the security policy has been derived from the Microsoft Windows 8, Microsoft Windows Server 2012 Security Target, the Assurance Activity Report, and Final ETR. The ST contains a more complete list of the security functionality that was assessed in the evaluation in Section 2.2.*

3.1 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.

3.2 Identification and Authentication

Each Windows user must be identified and authenticated based on administrator-defined policy (using password, network authentication token or a certificate on a smartcard) prior to performing any TSF-mediated functions. An interactive user invokes a trusted path in order to protect his I&A information. Windows maintains databases of accounts including their identities, authentication information, group associations, and privilege and logon rights associations. Windows account policy functions include the ability to define the minimum password length, the number of failed logon attempts, the duration of lockout, and password age.

3.3 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.

3.4 User Data Protection

Windows protects user data by enforcing several access control policies (Discretionary Access Control, Dynamic Access Control, Mandatory Integrity Control, web access and web content publishing access control) and several information flow policies (IPsec filter information flow control, Windows Firewall), as well as object and subject residual information protection. Windows uses access control methods to allow or deny access to named objects, such as files, directory entries, printers, and web content. Windows uses information flow control methods to control the flow of network traffic. Windows authorizes access to these resource objects through the use of security descriptors (an information set that identifies users and their specific access to resource objects), web permissions, network filters, and port mapping rules. Windows also protects user data by ensuring that resources exported to user-mode processes do not have any residual information.

3.5 Cryptographic Protection

Windows provides FIPS-140-2 validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement, 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 and a key isolation service designed to limit the potential exposure of secret and private keys. In addition to supporting its own security functions with cryptographic support, the TOE offers access to the cryptographic support functions for user application programs. Public key certificates generated and used by the TOE authenticate users and machines as well as user protect and system data in transit.

3.6 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. The Windows BitLocker features can be used to protect both fixed storage and removable USB storage volumes. Windows also includes some self-testing features that ensure the integrity executable TSF image and its cryptographic functions.

3.7 Session Locking

Windows provides the ability for a user to lock their session either immediately or after a defined interval. Windows constantly monitors the mouse and keyboard for activity and locks the workstation after a set period of inactivity. Windows allows an authorized administrator to configure the system to display a logon banner before the logon dialogue.

3.8 Trusted Path

Windows provides a trusted path for interactive session login as well as an IPsec trusted path when sending TSF data between machines that comprise a Windows deployment.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
- Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
- All connections to and from remote trusted IT systems and between physically-separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.
- Any modification or corruption of security-enforcing or security relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.
- The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
- All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.
- All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.
- It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

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 GPOSPP and performed by the evaluation team).
2. This evaluation covers only the specific product version identified in this document, and not any earlier or later versions released or in process.
3. 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 Architectural Information

This section provides a high level description of the TOE and its components as described in the ST and guidance documentation.

The diagram below depicts components and subcomponents of Windows. The components/subcomponents are large portions of the Windows operating system, and generally fall along process boundaries and a few major subdivisions of the kernel mode software.

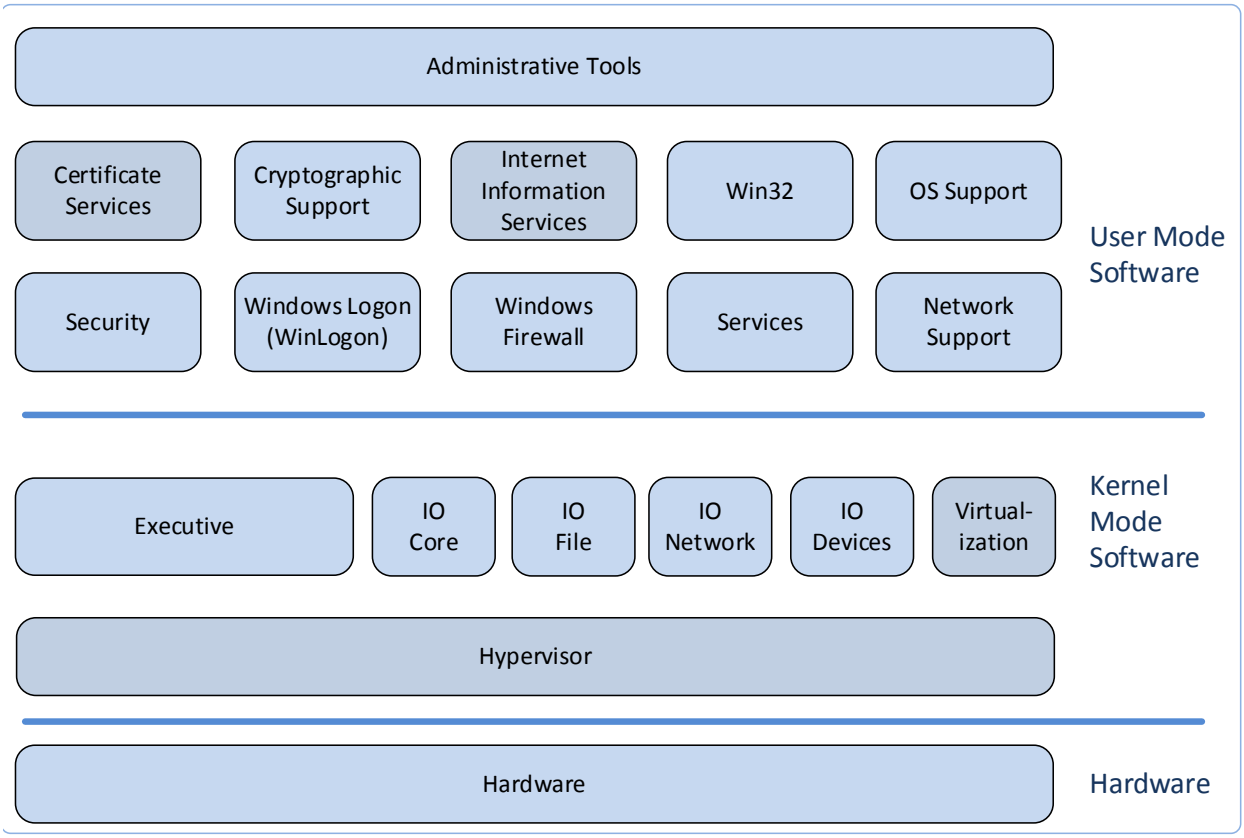

Figure 1 High-level Windows Architecture for Windows

- Administrative Tools Module

  - Administrative Tools Component: This component represents the range of tools available to manage the security properties of the TSF.
- Certificate Services Module
  - Certificate Server Component: This component provides services related to issuing and managing public key certificates (e.g. X.509 certificates).
- Windows Firewall Module
  - Windows Firewall Component: This component provides services related to network information flow control.
- Hardware Module
  - Hardware Component: This component includes all hardware used by the TSF to include the processor(s), motherboard and associated chip sets, controllers, and I/O devices.
- Kernel Software Module
  - Executive Component: This is the kernel-mode software that provides core OS services including memory management, process management, and inter-process communication. This component implements all the non-I/O TSF interfaces for the kernel-mode.
  - I/O System: This is the kernel-mode software that implements all I/O related services, as well as all driver-related services. The I/O System is further divided into:
    - I/O Core Component
    - I/O File Component
    - I/O Network Component
    - I/O Devices Component
  - Driver Virtualization: This is kernel-mode software that supports server virtualization as well as driver-related services to provide a virtualized set of device drivers to operating systems running on a guest partition. While this functionality was present in the system during the evaluation, the specific virtualization aspects were not explicitly tested.
  - Hypervisor: This is kernel-mode software executing in the root partition that manages virtual processors and address spaces to provide isolation between the root partition and guest partitions and isolation between guest partitions. It should be noted that although this functionality is present and operating in the evaluated configuration, its ability to provide isolation between multiple partitions was not tested during the evaluation; the evaluated configuration was a single partition running a specific Edition of the TOE.
- [Miscellaneous] OS Support Module
  - OS Support Component: This component is a set of processes that provide various other OS support functions and services.
- Network Support Module
  - Network Support Component: This component contains various support services for RPC, COM, and other network services.
- Security Module
  - Security Component: This component includes all security management services and functions.
- Services Module
  - Services Component: This is the component that provides many system services as well as the service controller that manages win32 services.

- Internet Information Services Module
  - IIS Component: This component provides services related to Web/HTTP requests.
- Win32 Module
  - Win32 Component: This component provides various support services for Win32 applications and the command console application.
- WinLogon Module
  - WinLogon Component: This component provides various interactive logon services to include interactive authentication, trusted path, session management and locking.
- Virtualization Module
  - This is user-mode software that supports the management of virtualization services as well as manage communication between guest partitions and the root partition. As indicated above, multiple partitions were not assessed nor tested during the evaluation; the evaluated configuration consisted of a single partition running the TOE.
- Cryptographic Support Module
  - Cryptographic Support Component: This component provides cryptographic services for use by the kernel and other components in a manner that keeps them distinct from other components of the TOE.

Physically, each TOE tablet, workstation, or server consists of an x86 or x64 architecture. The TOE executes on processors from Intel (x86 and x64) and AMD (x86 and x64). The specific devices listed in the ST are:

- Microsoft Surface Pro
- Dell Optiplex 755
- Dell Optiplex GX620
- Dell Latitude E6400
- HP XW9300
- Dell Precision M6300

A set of devices may be attached as part of the TOE:

- Display Monitors
- Fixed Disk Drives (including disk drives and solid state drives)
- Removable Disk Drives (including USB storage)
- Network Adaptor
- Keyboard
- Mouse
- Printer
- Audio Adaptor
- CD-ROM Drive
- Smart Card Reader
- Trusted Platform Module (TPM) version 1.2 or 2.0.

The TOE does not include any network infrastructure components.

6 Documentation

6.1 Product Guidance

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

- Microsoft Windows 8, Microsoft Windows Server 2012 Common Criteria Supplemental Admin Guidance
- On-line documentation referenced by the Supplemental Admin Guidance

The supplemental guidance document can be obtained my request from wincc@microsoft.com or from a customer's local technical account manager.

7 Product Testing

This section describes the testing efforts of the Evaluation Team. Part 2 of the GPOSPP outline the test approach to be followed for conformant TOEs. Because of the complexity and diverse nature of the implementations of the various SFRs in products (e.g., a Windows product vs. a Linux product), a two-pronged testing approach is described. First, there are generic tests associated with the SFRs in the PP. While these tests have varying degrees of specificity, it is expected that they will be refined by the evaluation team to apply to the specific implementation of the TOE. Second, there will be functionality associated with the SFRs that is implementation-specific and described in the TSS, but there is no explicit test in the corresponding assurance activity. Rather than leave this functionality untested, the GPOSPP mandates that test assertions be created to cover this functionality, and then that the evaluation team performs testing to show the test assertions to be true. This approach was followed by the evaluation for this evaluation.

Information in this section is derived from information contained in the Proprietary Assurance Activity Reports,[1] which documents the testing and analysis performed by the evaluation team. A more complete summary of the testing performed is contained in the *Microsoft Windows 8, Windows RT, Server 2012 Operating System Assurance Activity Report, v0.7, December 15th, 2014* (AAR).

Evaluation team testing was conducted at the Leidos (formerly SAIC) CCTL in Columbia, MD.

7.1 Developer Testing

The assurance activities in the GPOSPP do not specify any requirement for developer testing of the TOE, although it does provide direction on the use of existing developer tests by the evaluation team. For this evaluation, Microsoft made available their extensive suite—used in previous Windows evaluations—for use by the CCTL in performing evaluation team testing required by the GPOSPP.

7.2 Evaluation Team Independent Testing

The evaluation team performed the test coverage analysis specified in the GPOSPP as described above. The team prepared a test plan that included all the tests and interfaces identified through the analysis. The team executed the test plan and recorded results for all test runs, both successful and unsuccessful.

[1] The evaluation facility produced a series of 10 proprietary AARs totaling about 2500 pages. This information is summarized in the non-proprietary AAR referenced throughout this validation report.

The evaluation team performed the tests specified in the assurance activities of the GPOSPP. Testing included tests explicitly specified as SFR assurance activity tests in the profile as well as test cases to confirm test assertions derived from SFRs, TSS, and supporting evidence (e.g., the admin guide, pointers to on-line documents that support the TSS and admin guide). Additional tests were devised and executed in response to comments from the validation team, both from breadth of testing and depth of testing perspectives (these are documented in the proprietary validation issues document). A summary of all of the tests is given in the AAR, while the complete details of the evaluation team test and analysis effort is contained in the proprietary AARs.

The team tested the TOE in both standalone and distributed configurations. Testing consisted of executing both automated and manual tests. The evaluation team performed testing at Leidos facilities. The vendor test suites were used extensively to exercise the identified interfaces (see *Appendix B: Basic Functional Specification and Interfaces* of the ST). The vendor tests suites were largely automated. To assure the automated test results were consistent with the vendor's claims, the evaluation team analyzed the test documentation along with test results. Each automated test was delivered to the evaluation team with vendor-constructed test documentation. This test documentation had two main points of emphasis. The first was a summary of what the test does and what interfaces it touches. The second was instructions on how to run the test. The evaluation team ran each test according to the vendor provided instructions and monitored it in execution. Post-execution, the evaluation team analyzed the test output to verify: 1) all tests passed, 2) all interfaces that were claimed to be tested were actually tested, and 3) the TOE behavior was consistent with the vendor's claims in documentation. The test output reproduces assertions that were input to the test framework used in the automated tests. This framework took as input the interfaces tested, parameters to be used, etc. This gave the evaluation team knowledge and confidence that the documented claims were consistent with the automated tests.

The evaluation team used a sampling strategy to minimize redundant testing of TOE editions. The team identified ways in which the operating system editions are equivalent with respect to the SFRs in the GPOSPP. The team considered both global characteristics of the editions as well as features related to each set of security functional requirements. The team used equivalences between editions in the testing approach to provide complete testing while minimizing unnecessary duplicate tests of equivalent editions. The AAR presents a rationale for global equivalence of operating system editions that the validation team finds acceptable for this product. In addition, the test plan section for each group of SFRs presented an equivalency rationale related to the features specified by the SFRs. The testing strategy for each SFR group included tests on each system in a set of equivalent systems rather than testing on a single representative of the set.

One of the most-discussed issues during the writing of the GPOSPP (and one of the points of focus for the trial evaluation) concerned test coverage and functional testing that was more transparent, repeatable, and that minimized analysis by the evaluator when compared to then-current evaluation practices. Part 2 of the GPOSPP emphasizes a black box test approach for the functional testing aspect of the evaluation. In this evaluation, the vendor's test suite covered a variety of interfaces, but many of the covered interfaces were at a level below that presented to a user (and documented in Appendix B of the ST). The evaluation team, validation team, and vendor determined it was impractical and not cost-effective to require the evaluation team or vendor to re-write the tests at the interface level documented in the ST. Instead, the evaluation team conducted a limited analysis showing that the interfaces documented in the ST corresponded (invoked) the interfaces exercised in the test report. This was done largely by analysis of the TOE implementation using on-line documentation (for those cases where the Appendix B of the ST interface was shown to invoke the tested interface) and tools showing call-tree analysis for the Appendix B of the ST interface, which again showed that tested interface was being invoked.

The testing demonstrated the TOE satisfies the security functional requirements and assurance activities specified in the GPOSPP.

7.3 Penetration Testing

The GPOSPP, Part 2, outlines an approach to vulnerability analysis that calls for both CVEs and technology-specific flaws that are included in the PP to be addressed. However, due to time constraints, the list of CVE entries that was to accompany the GPOSPP was never produced. To address this issue, the evaluation team searched the NVD CVE list using search terms targeted to Windows operating system editions. Further, the team refined the search terms used for each SFR group (FDP, FIA, etc.). In some SFR groups, the nature of the function is such that searches apply across all security functional requirements in the group; for example, User Data Protection. In other SFR groups, the evaluation team was able to identify search terms specific to individual requirements.

The GPOSPP also does not include a list of technology-specific flaw hypotheses, which are also referenced in Part 2 of the PP. The evaluation team limited the search for vulnerabilities to target CVE searches and examination of evidence provided by the Developer.

The evaluation team generated flaw hypotheses based on examination of Microsoft evidence while performing assurance activities. The team documented their flaw hypotheses along with the analysis of potential flaws in each Proprietary SFR Assurance Activity Report.

The team then addressed each of the flaw hypotheses, and determined that there were no residual vulnerabilities from the list that they had created.

8 Evaluated Configuration

The evaluated version of the TOE consists of the following:

The following Windows Operating Systems (OS):

- Microsoft Windows 8 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 8 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 Standard Edition
- Microsoft Windows Server 2012 Datacenter Edition

The following security updates and patches must be applied to the above Windows 8 products:

- All critical security updates published as of October 2013.

The following security updates must be applied to the above Windows Server 2012 products:

- All critical security updates published as of October 2013.

TOE Hardware Identification: The following hardware platforms and components are included in the evaluated configuration:

- Microsoft Surface Pro
- Dell Optiplex 755
- Dell Optiplex GX620
- Dell Latitude E6400
- HP XW9300
- Dell Precision M6300

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the GPOSPP, in conjunction with version 3.1, revision 4 of the CC and the CEM.

The security assurance requirements contained in the OSPP are listed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ASE_INT.1	ST introduction
ASE_CCL.1	Conformance claims
ASE_SPD.1	Security problem definition
ASE_OBJ.2	Security objectives
ASE_ECD.1	Extended components definition
ASE_REQ.2	Derived security requirements
ASE.TSS.1	TOE summary specification
ADV_ARC.1	Security architecture description
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.3	Authorisation controls
ALC_CMS.3	Implementation representation CM coverage
ALC_DEL.1	Delivery procedures
ALC_FLR.3	Systematic flaw remediation
ALC_LCD.1	Developer defined life-cycle model
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.2	Vulnerability analysis

The GPOSPP, Part 2 provides a mapping of the assurance activities to the above SARs. The evaluation team produced an ETR for ASE and ALC components, as those were not covered by the assurance activities contained in the GPOSPP as stated in that mapping. The evaluation team produced a (non-proprietary) summary AAR, as well as detailed, proprietary AARs that covered each assurance activity. For each assurance activity, verdicts were given for each section (TSS, Functional Specification, Testing, Guidance, etc.) listed for the SAR in the GPOSPP.

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 GPOSPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

This section contains observations, recommendations, and caveats formulated by the validation team during the course of the evaluation and validation effort.

- The Administrative and User guidance for this evaluation is contained in *Microsoft Windows 8, Microsoft Windows Server 2012 Common Criteria Supplemental Admin Guidance* (Admin Guide). This document largely consists of pointers to existing Microsoft on-line documentation. The on-line documentation often contains an "Applies To" line listing the Windows versions and editions that that on-line page applies to. It is often the case that this Applies To line *does not* list the versions of Windows in the evaluated configuration (e.g., Windows 8, Server 2012). However, the vendor has stated that the fact that there is a pointer to the document in the Admin Guide to the on-line page indicates that the page is indeed valid for the evaluated configuration. Further, almost always a page that is pointed to by the Admin Guide contains additional pointers. The same rule applies to these pages (that is, ignore the "Applies To" line). However, the user also must ensure that the pointed-to pages are in scope of the evaluation. This is a cumbersome process that requires the reader to cross-reference the topic on the page with the information contained in the ST and (in some cases, where a determination whether the given feature is included or excluded cannot be made based on the information in the ST) the AAR, as well as any limitations stated in the Admin Guide.
- Additionally, there are many different methods for configuring or invoking the security functionality identified in the ST through various Windows interfaces. Only the interfaces listed in Appendix B of the ST were tested during the evaluation. Users should determine if the procedures or programs used in their operational environment use interfaces not listed in Appendix B. If so, those interfaces are candidates for further testing and/or analysis by the end user's information security organization.
- Windows Server 2012 supports various *Server Roles* as described in section 2.1.1.2 of the ST. These consist of additional capabilities to support various functions that the server performs. The evaluation team did not configure all of the server roles supported by Microsoft in their testing. The server roles that were configured are listed in the AAR. For server roles that provide additional functionality that may appear security-related (e.g., Virtualization), unless that functionality is directly related to an SFR in the ST, that functionality was not exercised during the evaluation.
- Section 2.2.3.6 of the ST discusses delta Certificate Revocation Lists. There are no specific requirements in the ST that call for delta CRLs to be tested, so while this mechanism may be been exercised in previous Windows evaluations, it was not exercised as part of this evaluation.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Microsoft Windows 8 and Windows Server 2012 Security Target, Version 1.0, December 19th, 2014.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003.
4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004.
5. General-Purpose Operating System Protection Profile, Version 3.9, January 15th, 2013.
6. Microsoft Windows 8 and Windows Server 2012 Security Target, Version 1.0, December 19th, 2014.
7. Microsoft Windows 8, Microsoft Windows Server 2012 Common Criteria Supplemental Admin Guidance, Version 1.0, December 11th, 2014.
8. Microsoft Windows 8, Windows RT, Server 2012 Operating System Assurance Activity Report, Version 0.7, December 15th, 2014.