National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 (version 1809) Hyper-V

Report Number:	**CCEVS-VR-VID11087-2021**
Dated:	**February 11, 2021**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
Attn: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

John Butterworth

Sheldon Durrant

Anne Gugel

Common Criteria Testing Laboratory

Leidos Inc.
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 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 carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 9, 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 Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 (version 1809) Hyper-V (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 (version 1809) Hyper-V (Hyper-V) was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in February 2021.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4]) and activities specified in the following documents:

- Protection Profile for Virtualization, Version 1.0, November 2016 [5]
- Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0, November 2016 [6]

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 product is a general-purpose operating system that includes a virtualization subsystem. The target of evaluation is the virtualization subsystem and those operating system components that are necessary for it to implement this functionality. The focus of the evaluation was on the product's conformance to the security functionality specified in [5] and [6].

The security functions specified in this Protection Profile and Extended Package include protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and Extended Package and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [7]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([10]) and the associated test report produced by the Leidos evaluation team ([9]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed Protection Profile and Extended Package and that the evaluation activities specified in [5] and [6] had been performed appropriately. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

- TD0139: Clarification of testing for FDP_RIP_EXT.2
- TD0206: Testing for Non-Existence of Disconnected Virtual Devices
- TD0230: ALC Assurance Activities for Server Virtualization and Base Virtualization PPs
- TD0247: FPT_VDP_EXT.1 Clarification for Assurance Activity
- TD0249: Applicability of FTP_ITC_EXT.1
- TD0250: Hypercall Controls – FPT_HCL_EXT.1 Clarification
- TD0264: Clarification of Auditable Events for FPT_RDM_EXT.1
- TD0360: AD Server configuration in FMT_MOF_EXT.1
- TD0363: Access Banner and applicability to programmatic interfaces
- TD0431: Modification to Cipher Suites for TLS
- TD0432: Corrections to FIA_AFL_EXT.1
- TD0443: FPT_VDP_EXT.1 Clarification for Assurance Activity
- TD0526: Updates to Certificate Revocation (FIA_X509_EXT.1)

1.2 Threats

The ST references the PP and EP to which it claims conformance for statements of threats that the TOE and its operational environment are intended to counter. Those threats, drawn from the claimed PP and EP, are as follows:

- If it is possible for data to leak between domains when prohibited by policy, then an adversary on one domain or network can obtain data from another domain. Such cross-domain data leakage can, for example, cause classified information, corporate proprietary information, or medical data to be made accessible to unauthorized entities.
- A malicious party attempts to supply the Administrator with an update to the product that may compromise the security features of the TOE.
- Malware running on the physical host must not be able to undetectably modify Virtualization System components while the system is running or at rest. Likewise, malicious code running within a virtual machine must not be able to modify Virtualization System components.
- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Vulnerabilities in 3rd party software can lead to VMM compromise. Where possible, the VS should mitigate the results of potential vulnerabilities or malicious content in third-party code.
- Failure of security mechanisms could lead to unauthorized intrusion into or modification of the VMM or bypass of the VMM altogether.

- The hosting of untrusted or malicious domains by the VS cannot be permitted to compromise the security and integrity of the platform on which the VS executes.
- A user may gain unauthorized access to the TOE data and TOE executable code. 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 threat of weak cryptography may arise if the VMM does not provide sufficient entropy to support security-related features that depend on entropy to implement cryptographic algorithms.
- The Virtualization System itself is generally part of a larger enterprise network and must be updated and patched as a normal part of enterprise network operations. Such basic network hygiene is more difficult if the enterprise network is unmanageable

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 (version 1809) Hyper-V
Sponsor & Developer:	Microsoft Corporation One Microsoft Way Redmond, WA 98052
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	February 15, 2021
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
Protection Profile/Extended Package:	Protection Profile for Virtualization, Version 1.0, November 17, 2016 Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0, November 7, 2016
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Justin Fisher Allen Sant Kevin Steiner
Validation Personnel:	John Butterworth Sheldon Durrant Anne Gugel

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 ST and the ETR.

3.1 Security Audit

The TOE 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. In the context of this evaluation, the protection profile requirements cover generating audit events, authorized review of stored audit records, and providing secure storage for audit event entries both on the TOE and in its operational environment.

3.2 Cryptographic Support

The TOE provides validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, and random number generation. The TOE implements these functions in support of IPsec, TLS, and HTTPS protocol implementation. The TOE also ensures that its Guest VMs have access to entropy data so that virtualized operating systems can ensure the implementation of strong cryptography.

3.3 User Data Protection

The TOE makes certain computing services available to Guest VMs but implements measures to ensure that access to these is granted on an appropriate basis and that these interfaces do not result in unauthorized data leakage between Guest VMs and the TOE or between multiple Guest VMs.

3.4 Identification and Authentication

The TOE offers several methods of user authentication, which includes X.509 certificates needed for trusted protocols. The TOE implements password strength mechanisms and ensures that excessive failed authentication attempts using methods subject to brute force guessing (password, PIN) results in lockout behavior.

3.5 Security Management

The TOE includes several functions to manage security policies. Access to administrative functions is enforced through administrative roles. The TOE also has the ability to support the separation of management and operational networks and to prohibit data sharing between Guest VMs.

3.6 Protection of the TSF

The TOE implements various self-protection mechanisms to ensure that it cannot be used as a platform to gain unauthorized access to data stored on a Guest VM, that the integrity of both the TSF and its Guest VMs is maintained, and that Guest VMs are accessed solely through well-documented interfaces.

3.7 TOE Access

In the context of this evaluation, the TOE allows an authorized administrator to configure the system to display a logon banner before the logon dialog.

3.8 Trusted Path/Channels

The TOE implements IPsec, TLS, and HTTPS trusted channels and paths for the purpose of remote administration, transfer of audit data to the operational environment, and separation of management and operational networks.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The platform has not been compromised prior to installation of the Virtualization System.
- Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in the claimed PP and EP [5] and [6] and performed by the evaluation team).
- 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.
- The evaluation of security functionality of the product was limited to the functionality specified in the Security Target [7].
- The TOE consists of software and does not rely on the operational environment for any supporting security functionality.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in section 6 of this Validation Report.

5 TOE Evaluated Configuration

5.1 Evaluated Configuration

The TOE is Microsoft Windows Hyper-V on one of the following operating system versions and editions:

- Microsoft Windows Server Standard edition, version 1909
- Microsoft Windows Server Datacenter edition, version 1909
- Microsoft Windows Server 2019 Standard edition
- Microsoft Windows Server 2019 Datacenter edition
- Microsoft Windows 10 Enterprise edition, version 1909 (64-bit version)

TOE Versions:

- Windows Server: build 10.0.18363 (also known as version 1909)
- Windows Server 2019: build 10.0.17763 (also known as version 1809)
- Windows 10: build 10.0.18363 (also known as version 1909)

The following security updates must be applied for:

- Windows Server and Windows 10: all critical updates as of December 31, 2020
- Windows Server 2019: all critical updates as of December 31, 2020

The tested configuration of the TOE relied on the following non-TOE hardware:

- Dell PowerEdge R640
- Dell PowerEdge R7425
- Microsoft Surface Book 2

The TOE is configured in accordance with the evaluated configuration guidance specified in section 6 of this VR.

5.2 Excluded Functionality

All product functionality that is not claimed by the Security Target as part of achieving exact conformance to the claimed PP and EP is excluded from the evaluation scope. In particular, the TOE is the Hyper-V subsystem of the Windows operating system and includes dependencies from the operating system where necessary to address required functionality. However, the general-purpose operating system functionality of Windows is not part of the TOE.

6 Documentation

Microsoft offers guidance documentation describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with each TOE version is as follows:

- Operational and Administrative Guidance, Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 version 1809 Hyper-V [8]

This is also provided for initial setup purposes. To use the product in the evaluated configuration, the product must be configured as specified in this guidance. Note that this guidance also references external links to existing Microsoft documentation where appropriate rather than duplicating materials that are already available to users.

7 Independent Testing

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

- Microsoft Hyper-V Common Criteria Test Report and Procedures for Virtualization PP [9]

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

- Assurance Activities Report for Microsoft Hyper-V [10]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance the *Protection Profile for Virtualization* [5] and the *Protection Profile for Virtualization Extended Package Server Virtualization* [6].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in [5] and [6]. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for [5] and [6] were fulfilled.

7.1 Test Configuration

The evaluated version of the TOE consists of several versions of Microsoft Windows with Hyper-V running on separate hardware devices.

The TOE must be deployed as described in section **Error! Reference source not found.**.1 of this Validation Report and be configured in accordance with the Common Criteria Operational and Administrative Guidance [8].

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.

7.2 Vulnerability Analysis

The evaluation team performed a vulnerability analysis following the processes described in the claimed Protection Profile and Extended Package and using the flaw-hypothesis methodology. This included a search of public vulnerability databases as well as those maintained by the product vendor. These searches were performed during the evaluation on November 19, 2020, and January 15, 2021. Full results and analysis were documented in [11].

The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and the Microsoft Security Research Center (https://msrc.microsoft.com/update-guide).

The following search terms related to Windows components and features were used:

1. BitLocker
2. Microsoft Security Event Log
3. Microsoft Windows Event Log Service
4. Microsoft Windows Get-EventLog
5. Microsoft Windows Local Security Authority server
6. Windows Access Control
7. Windows Access Control List
8. Windows ACE
9. Windows ACL
10. Windows Active Directory
11. Windows Active Directory Certificate Services
12. Windows Attribute Initialization
13. Windows Authentication
14. Windows Authentication Failure
15. Windows Authentication Feedback
16. Windows bcrypt
17. Windows Certificate Authority
18. Windows Certificate Management
19. Windows Certificate Services
20. Windows CNG
21. Windows crypto
22. Windows DAC
23. Windows DACL
24. Windows default
25. Windows Discretionary Access Control
26. Windows Discretionary Control
27. Windows Dynamic Access
28. Windows Encryption
29. Windows Enlightenment
30. Windows Event Viewer
31. Windows Firewall
32. Windows Groups
33. Windows Guest
34. Windows Hyper-V
35. Windows Hypervisor
36. Windows Integrity Control
37. Windows Integrity Control Policy

38. Windows IPsec
39. Windows Logon
40. Windows Management
41. Windows ncrypt
42. Windows NTP
43. Windows Object
44. Windows Parent
45. Windows Partition
46. Windows Password
47. Windows Password Entry
48. Windows Password Management
49. Windows PKI
50. Windows Privilege
51. Windows Privileges
52. Windows Remote Authentication
53. Windows Remote Desktop
54. Windows Remote Management
55. Windows Residual Data
56. Windows Role Management
57. Windows Roles
58. Windows SACL
59. Windows Screen Lock
60. Windows Security Descriptor
61. Windows Security Management
62. Windows SID
63. Windows Smart Card
64. Windows Synthetic
65. Windows Time Service
66. Windows TLS
67. Windows User Identity
68. Windows User Lockout
69. Windows Virtual Switch
70. Windows Virtualization
71. Windows VMBus
72. Windows x.509
73. Winlogon

The following searches were performed based on the full names of the OS platform versions within the logical scope of the TOE:

- Windows 10 Version 1909 (November 2019 Release)
- Windows Server Version 1909 Standard Edition (November 2019 Release)
- Windows Server Version 1909 Datacenter Edition (November 2019 Release)
- Windows Server 2019 Standard Edition (November 2018 Update)

- Windows Server 2019 Datacenter Edition (November 2018 Update)

Vulnerability searches were also conducted using the following CPEs that correspond to the OS platform versions listed above:

- cpe:/:microsoft:windows_server_2019
- cpe:/:microsoft:windows_10:1909
- cpe:/:microsoft:windows_server_2016:1909

Note that CPEs are not granular to the specific licensed editions of Windows (Enterprise, Standard, Datacenter, etc.). Therefore all findings for a particular CVE are assumed to apply to all Windows editions unless explicitly specified otherwise.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 5 of the CC and CEM:

- Protection Profile for Virtualization, Version 1.0, November 2016 [5]
- Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0, November 2016 [6]

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

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 PP and EP, 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 2: 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
ALC_TSU_EXT.1	Timely security updates
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). 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 the devices, 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.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

10 Annexes

Not applicable

11 Security Target

The ST for this product’s evaluation is *Microsoft Windows Server Microsoft Windows 10 version 1909 (November 2019 Update) Microsoft Windows Server 2019 version 1809 Hyper-V Security Target*, Version 0.02, January 8, 2021 [7].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

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 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017

[5] Protection Profile for Virtualization, Version 1.0, November 17, 2016

[6] Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0, November 17, 2016

[7] Microsoft Windows Common Criteria Evaluation Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update) Microsoft Windows Server 2019 (version 1809) Hyper-V Security Target, Version 0.2, January 8, 2021

[8] Operational and Administrative Guidance, Microsoft Windows Server, Windows Server 2019, and Windows 10 Hyper-V (version 1909 / November 2019 Update), January 15, 2021

[9] Microsoft Windows 10 Hyper-V Common Criteria Test Report and Procedures for Virtualization PP, Version 1.1, February 8, 2021

[10] Assurance Activities Report For Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 (version 1809) Hyper-V, Version 1.0, February 8, 2021

[11] Microsoft Windows Server Microsoft Windows 10 version 1909 (November 2019 Update) Microsoft Windows Server 2019 version 1809: Hyper-V Vulnerability Analysis, Version 1.1, January 15, 2021