Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ver.3.1 rel. 5

Certificato n. *(Certificate No.)*	04/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/14/2024/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	2 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	IBM PowerVM 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9
Sviluppatore *(Developer)*	IBM Corporation
Tipo di Prodotto *(Type of Product)*	Sistemi Operativi (Operating Systems)
Conformità a PP *(PP Conformance)*	Protection Profile for Virtualization. Ver.1.1, PP-Module for Server Virtualization Systems. Ver. 1.1, Functional Package for Transport Layer Security (TLS). Ver. 1.1, Functional Package for Secure Shell (SSH). Ver. 1.0, CC Parte 3 estesa
Funzionalità di sicurezza *(Conformance of Functionality)*	Funzionalità conformi a PP, CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 2 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando Metodologia Comune per la Valutazione di Sicurezza della tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Organismo di Certificazione della Sicurezza Informatica

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM PowerVM 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9

OCSI/CERT/ATS/14/2024/RC

Version 1.0

2 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First Issue	02/02/2026

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AIX	Advanced Interface Executive
BMC	Baseboard Management Controller

CLI	Command Line Interface
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
DES	Data Encryption Standard
ECC	Elliptic-curve Cryptography
ESS	Entitled Software System
FTP	File Transfer Protocol
FTPS	FTP Secure
FW	Firmware
GUI	Graphical User Interface
HMC	Hardware Management Console
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IBM	International Business Machines
LPAR	Logical Partition
RSA	Rivest-Shamir-Adleman
RTAS	Run Time Abstraction Services
SAN	Storage Area network
SHA	Secure Hash Algorithm
SSH	Secure SHell
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
vENT	Virtual Ethernet
VIOS	Virtual Input/Output System
VM	Virtual Machine
vSCSI	Virtual Small Computer Serial Interface

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 - Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[CCGUIDE] IBM PowerVM 1060.10 with VIOS 4.1.1 for Power10 and HMC 10.3.1062.1 for Power 9 Evaluated Configuration Guide version 1.7 Jul 1, 2025.

[ETRv2] Final Evaluation Technical Report RACF for IBM PowerVM 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9, atsec information security s.r.l., v.2.0, 28 November 2025.

[MOD_SV] PP-Module for Server Virtualization Systems, Version 1.1, 14 June 2021.

[PKG_SSH] Functional Package for Secure Shell (SSH). Version 1.0, 13 May 2021.

[PKG_TLS] Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019.

[ST] IBM PowerVM 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9 Security Target version 2.0, 21 July 2025.

[VPP] Protection Profile for Virtualization, Version 1.1, 14 June 2021.

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 8 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**IBM PowerVM 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9**", developed by International Business Machines (IBM) Corporation.

IBM PowerVM FW 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9 (also referred to in the following as **IBM PowerVM**) facilitates the sharing of hardware resources by disparate applications. The TOE is based on the concept of a "hypervisor" that is designed to instantiate "partitions", each with its own distinct resources, that each appear to their hosted applications as a completely functional underlying platform.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3, NIS5]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance provided for the evaluation assurance level defined by the SARs included in the PP [VPP] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named "IBM PowerVM FW 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	IBM PowerVM FW 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9
Security Target	IBM PowerVM 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9 Security Target, v.2.0 July 21st , 2025 [ST]
Evaluation Assurance Level	PP conformant with the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1 ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security s.r.l.
CC version	3.1 Rev. 5
PP conformance claim	[VPP]: Protection Profile for Virtualization. Version 1.1 [MOD_SV]: PP-Module for Server Virtualization Systems. Version 1.1 [PKG_TLS]: Functional Package for Transport Layer Security (TLS). Version 1.1 [PKG_SSH]: Functional Package for Secure Shell (SSH). Version 1.0.
Evaluation starting date	June 26th, 2024
Evaluation ending date	November 28th, 2025

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are

fulfilled and, in the configuration, shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description refer to the Security Target [ST].

The Target of Evaluation (TOE) is IBM PowerVM FW 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9 with the software components as described in Table 3, sect. 9.1.1.

The TOE facilitates the sharing of hardware resources by disparate applications (e.g., AIX, IBM i, Linux). The TOE is based on the concept of a "hypervisor" that is designed to instantiate "partitions", each with its own distinct resources, that each appear to their hosted applications as a completely functional underlying platform. The TOE is implemented to prevent interference among these partitions, known as Logical PARtitions (LPARs) and to prevent simultaneous sharing of storage and other device resources. VIOS allows partitions access-controlled sharing of individual storage and network devices. The TOE is agnostic to the application running in an LPAR.

Both PowerVM and VIOS are configured and managed by the Hardware Management Console (HMC). HMC provides functionality necessary for administrative personnel to manage the allocation of resources to the configured partitions

For a more detailed description of the TOE, please refer to sections 1.4 e 1.5 of the Security Target [ST]. Main aspects are described in the following sections.

7.3.1 TOE architecture

The TOE comprises the PowerVM Hypervisor (PHYP), VIOS, and HMC: it consists of multiple architectural components.

The components expose several interfaces both externally and internally.

The external interfaces the Hypervisor interfaces as well as the hardware instructions available to applications. There is also an operator panel where basic, non-security related operator functions can be performed by a user with direct physical access to the TOE.

The internal interfaces, specifically those not also available externally, include the Flexible Service Processor interface to the Hypervisor. I/O represents the physical I/O slots either integrated into the hardware drawers or I/O drawers external to the server. The I/O adapters allow for the connection of disk, network, Storage Area Network (SAN), tape, and other individual I/O devices.

The physical boundaries can then be broken down into individual logical components. For example, a physical drawer may contain 8 different I/ O devices; these individual devices are assigned by the HMC to the configured virtual machines (partitions).

7.3.2 TOE security features

The primary security features of the TOE are:

- Auditing
- Cryptographic Support
- User Data Protection
- Identification and authentication

- Security management
- TSF protection
- TOE Access Banner
- Trusted Path/Channels

7.3.2.1 Auditing

The TOE provides an audit capability that allows audit records to be generated for security critical events specified in FAU_GEN.1. The audit records are generated through the HMC and VIOS and stored locally as well as transferred to an external audit server protected via SSH.

The VIOS records audit events pertaining to connections between the VMs and virtual or physical networking components.

The HMC records all audit events listed in FAU_GEN.1. Audit records are viewable by authorized administrators and are protected from unauthorized modification and deletion.

7.3.2.2 Cryptographic Support

The TOE provides cryptographic support using OpenSSL, OpenSSH, and Java cryptographic modules implemented in the TOE.

The TOE uses the OpenSSL version 1.1.1k cryptographic module on the HMC for the following services:

- RSA key generation for X.509 certificates and user and peer authentication;
- RSA key generation for SSH user and peer authentication;
- HMC trusted updates using published hash.

The TOE uses the OpenSSL version 3.1.3 cryptographic module on the Server and the Baseboard Management Controller (BMC) for the following services:

- Server trusted updates using RSA digital signatures.

The TOE uses the Java version 17.0.10 cryptographic module for the following services:

- Trusted paths/channels for incoming connections from the remote administrator through HMC GUI to the HMC over HTTPS/TLS 1.2;
- RSA key generation for use by RSA and ECC key establishment schemes in the TLS 1.2 protocol.

The TOE uses the OpenSSH version 8.0p1-19.el8.2 cryptographic library for the following services:

- Trusted channel for incoming and outgoing connections to the external audit storage via Secure File Transfer Protocol (SFTP) using the Secure Shell version 2 (SSHv2) protocol;
- Trusted path for incoming connection from the remote administrator through HMC Command Line Interface (CLI) to the HMC using the Secure Shell version 2 (SSHv2) protocol;
- ECC key generation for use by EC-Diffie-Hellman in the SSHv2 protocol;
- RSA key-based authentication.

7.3.2.3 User Data Protection

Hypervisor

The Hypervisor manages the association of CPUs, memory, and I/O devices, in a relatively static environment, with partitions containing operating system instances. Memory and I/O devices can be assigned to single partitions and when assigned are accessible only by the partition (including OF/RTAS (Run Time Abstraction Services) and the OS running in the partition).

CPUs can also be assigned a single partition, and only that partition (and occasionally the TOE) can use that CPU. CPUs can also be configured to be shared among a collection of partition (shared processor partition or also called micropartitions) and the Hypervisor will save/restore the hardware register state when switching between partitions. Partitions have no control over the resources they are assigned.

The Hypervisor receives the partition management information from the HMC when it is being configured.

VIOS

VIOS manages the association of partitions to virtualized storage and network devices and the association of virtualized storage and network devices to physical storage and network devices. Through the HMC, an administrator assigns a set of physical storage and network devices to the VIOS partition. The administrator then creates virtual storage and network devices in VIOS, maps the physical devices to the virtualized devices, and maps the vSCSI (virtual Small Computer Serial Interface) and vENT (virtual Ethernet) to other partitions on the system. These other partitions access the virtualized storage and virtual networking controlled by VIOS. VIOS provides the separation protection between the virtualized storage and virtual network devices so that one partition cannot access another partitions information.

7.3.2.4 Identification and Authentication

Partitions are implicitly identified by internal numerical identifiers associated with partitions (using internal data structures) as they are defined. Being implicitly identified by the TOE, partitions have no need, nor means, to identify themselves. Furthermore, the identification of a partition is guaranteed by the Hypervisor. The Hypervisor identifies administrators for configuring and managing partitions and VIOS devices. Administrators use the HMC console to configure and manage the TOE. Administrators can connect to the HMC console via the web-based GUI over HTTPS or via the CLI over SSH. **In the evaluated configuration, only local user authentication is supported**.

7.3.2.5 Security Management

The TOE configuration and management occurs via the interface to the HMC console. Administrators can configure and manage the security functions used by the TOE. The TOE supports the separation of management and operational network traffic through separate physical network.

7.3.2.6 Protection of the TSF

The components of the TOE protect themselves using the domains provided by the processors. The Hypervisor operates in the privileged domain and the partitions, like VIOS, operate in the unprivileged domain. This allows the Hypervisor to protect itself as well as the resources it makes selectively available to the applicable partitions. Beyond protecting itself and its resources, the TOE is also designed such that when the hardware that supports a partition fails, the other partitions will

continue uninterrupted. Additionally, the TOE provides trusted software updates via a published hash (HMC) and digital signature (Server).

7.3.2.7 TOE Access Banner

The TOE provides the capability of displaying of an advisory warning message regarding unauthorized use of the TOE before establishing an administrator session (i.e., the HMC Console).

7.3.2.8 Trusted Path/Channels

The TOE provides protected communications between itself and the following external entities.

- Connections using HTTPS/TLS
  - Connection between the remote administrator and the HMC through the HMC GUI;
- Connections using SSH
  - Connection between the remote administrator and the HMC through the HMC CLI;
  - Connection between the HMC and the external audit storage over SFTP.

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage of the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 9 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims exact conformance the following:

- [VPP]: Protection Profile for Virtualization. Version 1.1;
- [MOD_SV]: PP-Module for Server Virtualization Systems. Version 1.1;
- [PKG_TLS]: Functional Package for Transport Layer Security (TLS). Version 1.1;
- [PKG_SSH]: Functional Package for Secure Shell (SSH). Version 1.0.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected or derived from CC Part 3 [CC3]. This includes ALC_TSU_EXT.1.1 - Timely Security Updates, as defined in [VPP].

All the Security Functional Requirements (SFRs) have been selected or derived by extension from CC Part 2 [CC2].

It is possible to refer to the Security Target [ST] for the description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFRs) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and [NIS5] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

Moreover, all the activities requested by the [VPP] protection profile have been performed.

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security s.r.l.

The evaluation was completed on November 28th, 2025 with the issuance by LVS of the Evaluation Technical Report v.2 [ETRv2] that was approved by the Certification Body on 22 December 2025. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in “Annex B – Evaluated configuration”.

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report v.2 [ETRv2] issued by the LVS atsec information security s.r.l. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "IBM PowerVM FW 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level defined by the SARs included in the PP [VPP], with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance components reported in defined by the SARs included in the PP [VPP] (In *Italics* are reported the extended assurance components).

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Basic functional specification	ADV_FSP.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Labelling of the TOE	ALC_CMC.1	Pass
TOE CM coverage	ALC_CMS.1	Pass
Timely Security Updates	*ALC_TSU_EXT.1*	*Pass*
Test	**Class ATE**	Pass
Independent testing - Conformance	ATE_IND.1	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability survey	AVA_VAN.1	Pass

Table 1 Final verdicts for assurance requirements

8.2 Additional assurance activities

The Protection Profile for Virtualization [VPP] includes additional assurance activities specific to the TOE technology type, and are required for exact conformance to the PP.

The Evaluators used for the PP assurance activities a notation similar to assurance components of existing CC assurance classes.

The objective of these sub-activities is to determine whether the requirements of the assurance activities included in the PP are met. summarizes the final verdict of the PP assurance activities carried out by the LVS

Table 2 summarizes the final verdict for each assurance activity of the PP carried out by the LVS.

PP assurance activities[1]		**Verdict**
ASE: Security Target evaluation	ASE_BVPP.1	Pass
	ASE_SVPPM.1	Pass
	ASE_TLSPKG.1	Pass
	ASE_SSHPKG.1	Pass
AGD: Guidance documents	AGD_BVPP.1	Pass
	AGD _SVPPM.1	Pass
	AGD _TLSPKG.1	Pass
	AGD _SSHPKG.1	Pass
ALC: Life cycle support	ALC_BVPP.1	Pass
ATE: Test	ATE_BVPP.1	Pass
	ATE _SVPPM.1	Pass
	ATE _TLSPKG.1	Pass
	ATE _SSHPKG.1	Pass
AVA: Vulnerability assessment	AVA_BVPP.1	Pass

Table 2 – Final verdict for additional assurance activities

8.3 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

[1] Activities with the _BVPP, _SVPPM, _TSLPKG, _SSHPKG extension were entered by the lab to clearly organize the activities from the VPP's "Assurance Activities" and related to activities for verification SFRs from PP-Module for Server Virtualization Systems [MOD_SV], Functional Package for TSL [PKG_TLS] and Functional Package for SSH [PKG_SSH] respectively.

Potential customers of the product "IBM PowerVM FW 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "*Objectives for the Operational Environment*" specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.2 of the Security Target [ST] shall be satisfied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A – Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE [CCGUIDE].

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

9.1.1 Scope of TOE supply

The following table contains the item that comprise the different elements of the TOE.

No	Type	Identifier	Release/Version	Form of Delivery
1	PowerVM firmware on Power10 CPU	PowerVM Hypervisor	01ML1060_064_053 (FW1060.10)	Digital delivery
2	HMC firmware on Power9 CPU	Hardware Management Console	10.3.1062.1	Digital delivery
3	VIOS	Virtual I/O server	4.1.1.0	Digital delivery
4	Doc.	IBM PowerVM 1060.10 with VIOS 4.1.1 for Power10 and HMC 10.3.1062.1 for Power 9 Evaluated Configuration Guide Jul 1st, 2025 [CCGUIDE]	1.7	Electronic

Table 3 - TOE Deliverables

9.1.2 Delivery procedure

Section 4.2 "Hardware Management Console installation" of [CCGUIDE] instructs the user on how to obtain HMC Releases in a secure way on the HMC Power 9 Appliance. It specifies that the HMC Power 9 Appliance will be pre-loaded with the Base HMC Release 10.3.1050.0 version as part of Manufacturing. The following installation steps are provided:

1. on power on, the HMC will be loaded with version 10.3.1050.0;
2. user can login with the default user “hscroot” and default password “abc123”. On the first successful login the HMC will mandate the user to change the password. User can choose new password and proceed to next steps;
3. with the new credentials HMC will guide the User to set the Network Settings for the HMC;
4. to update the HMC to 10.3.1062.1 User has to update the following “*Update drivers*”

- first update image 10.3.1062.0;
- then update image 10.3.1062.1.

To update the system in the evaluated configuration, **the administrator must follow the guidance provided**. First of all, the image must be downloaded at the *IBM Fix Central URL*[2]. After that the image (10.3.1062.1 in the example below) can be installed with the following command:

updhmc -t disk -f /home/hmcsuperadmin/MF71728-10.3.1062.1-2506170641-ppc64le.iso -r

Section 4.4 "System Firmware Installation" of [CCGUIDE] provides instructions on how to obtain system firmware for Power10 in a secure way. It provides guidance on how to install the evaluated firmware on the user's machine. After downloading it at the IBM fix central portal, the following steps must be followed:

1. from the HMC, In the navigation area, click the Resources icon, and then select All Servers;
2. select the server for which you want to update system information and click Actions > Updates
3. choose your source file location;
4. select Change Licensed Internal Code > for the Current Release or to a new Release based on the currently installed release;
5. select an action from the list and click Ok;
6. when you complete this task, click Close.

Chapter 4.5 "VIOS installation" of [CCGUIDE] guides the user in downloading and obtaining the flash image for VIOS in a secure way. It guides the user on how to download and install the VIOS image:

1. go to the Entitled Systems Support (ESS)[3]
2. (if the customer have never been on the site before, must be registered with the "attach" procedure to the IBM Customer Number);
3. select **My entitled software** for the initial ESS webpage;
4. enter Select the OS category by toggling the "Category" field (i.e., AIX, IBM i or Linux Linux) and then specify OS level version by interacting with the "Group" field (e.g., "Category: IBM i", "Group: 7.6"). For reference, see Figure 2 in chapter 5 "Appendix" of [CCGUIDE];
5. roll through the various software offerings and select 5765-VE4 PowerVM V4
6. select package 2282: IBM PowerVM V4 / VIOS 2282 v04.01.01,ENU, DVD
7. agree to the terms and conditions for the software download;
8. select HTTPS for download method;
9. select Virtual_IO_Server_Base_Install_4.1.1.0_DVD_122024_122024_LCD8298701.iso file;
10. after uploading the above file to the HMC, follow the procedure outlined in link (https://www.ibm.com/docs/en/power10?topic=mvis-activating-virtual-io-servers)

[2] https://www.ibm.com/support/fixcentral
[3] https://www.ibm.com/servers/eserver/ess/landing/index.html

In addition, section 4.5.1 "Installing iFixes on VIOS" of [CCGUIDE] provides instructions on how to install iFixes for VIOS to ensure it is not vulnerable to public CVEs. The iFix and its digital signature can be downloaded using the following command:

emgr_download_ifix -L <https_link> -P /tmp/

After that, the ifix's signature can be verified and the update can be installed with the following command:

/usr/sbin/emgr_sec <ifix_name.Z>

On top of the aforementioned fix, also other fixes, listed in section 4.5.1 of [CCGUIDE] must be installed.

Since the HMC Power 9 Appliance is pre-loaded with the Base HMC Release 10.3.1050.0, two updates must be executed to bring the TOE into the evaluated configuration. Firstly, to 10.3.1062.0 and then to 10.3.1062.1.

Section 4.2 of [CCGUIDE] specifies that the HMC images to be installed are:

- update: MF71722-10.3.1062.0-2505290127-ppc64le.iso
- update: MF71728-10.3.1062.1-2506170641-ppc64le.iso

The user can validate the package information for the downloaded iso update images by following the instructions provided in the "Step to verify the hash for the HMC Update driver" section of the chapter 4.2 "Hardware Management Console Installation" of [CCGUIDE] :

For reference, the hash for the HMC images are the following:

- MF71722: 0b3483e58de897e913b7426add5aca96fb203460
- MF71728: 26b7e8d251df7e70ce4f00d73759b302b493611c

If the user wanted to manually check the integrity and authenticity of the **system firmware** downloaded iso, he can follow the instructions provided in section 4.4 of [CCGUIDE]:

1. upload the image to the HMC;
2. from the directory containing the image, run the following command: sha256sum <image>
3. compare the resulting hash with the expected value to ensure integrity.

For reference, [CCGUIDE] provides the following hash for the system firmware iso:

826871c1446a625f0e6dff6278892cebb34f5151645e403d959b05f98f7e1138.

If the user wanted to manually check the integrity and authenticity of the **VIOS** downloaded iso, he can follow the instructions provided in section 4.4 of [CCGUIDE] :

1. upload the image to the HMC;
2. from the directory containing the image, run the following command: sha256sum <image>
3. compare the resulting hash with the expected value to ensure integrity.

For reference, [CCGUIDE] provides the following hash for the VIOS iso:

f85b70ea32c510e2dbcf6e4f2064a9aa7b34223e6ab5b497c726343802cdba9.

The evaluated configuration also requires for some **iFixes** to be installed. All iFixes, as stated in chapter 4.5.1 "Installation of iFixes within VIOS" of [CCGUIDE], are digitally signed by IBM. The

public keys that allow for the verification of the signature of the iFixes are provided with the evaluated configuration.

Every iFix can be downloaded and installed following the guidance provided in section 4.5.1 of [CCGUIDE].

All the hashes for the iFixes are provided as follows:

- SUMA_IFIX_CC: *3e754bbd6881badb6b9bd8ec65ff87c57bdc0c827c65e48d4223e0216edb609e*
- openssl_fix44: *dc6d5d0e1fb79c63ccea079a50c44fdc3c2c7a380c9c51d4f228085621be8fd2*
- python_fix14: *7263fb732756274afd2ba08cb6f6fc2ec14add427bcc11e9a8a654d98d481cf1*
- openssh_fix18: *aeb8c08023719fcab155c7c25f08ce42e5a8880b19d7b11873e43ea4ca669c33*
- nim_fix: *f53fff566425dad9e7bcea8f94add4e743e900ae2d822e1962644d13dae246d4*
- libxml2_fix7: *7896479ce2acbac2aebcb4d957d1b2c00842c27e10184dd1ec175d0bcb509540*
- dbg_ccssha: *31099629c04c7bd6b3e0a79746b4ba6c15a69361d275a62d21daa4d961d9265d*
- tmux35as0a: *fb73e8a7c126fe97ccc76a09404dd1fd47c104d0a50ffaa7e6e0ae7d85198531*

9.2 Identification of the TOE by the user

Chapter 4 of [CCGUIDE] provides information on how to identify the version of the TOE, respectively chapter 4.2 for the HMC component, chapter 4.4 for the Server component, and finally 4.5 for the VIOS component.

Chapter 4.2 of [CCGUIDE] instructs the user on how to query the HMC's current version:

lshmc -V

The same goes for chapter 4.4 where instructions are given on how to verify the level of firmware installed on the TOE:

1. From the HMC, In the navigation area, click the Resources icon, and then select All. Servers.
2. Select the server for which you want to view system information.
3. In the menu pod, expand Actions and then expand Updates.
4. Select View system information
5. In the Specify LIC Repository window, select None – Display current values and click ok.

The same goes for chapter 4.5 which instructs the user on how to verify the current level of firmware installed on the TOE:

1. From the HMC, In the navigation area, click the Resources icon, and then select All Servers.
2. Select the server for which you want to view system information.
3. In the system menu, select Virtual IO Server
4. Select the VIOS partition
5. Under VIOS Properties, the version is displayed.

Ultimately, since the guidance documentation is also part of the TOE as stated in the [ST], the Evaluators also checked that instructions are provided on how to download the [CCGUIDE].

9.3 Installation, configuration and secure usage of the TOE

TOE installation, configuration and secure usage should be done by following the instructions in the appropriate sections of the guidance documentation [CCGUIDE] provided with the product to the customer.

In particular, Section 4.3 "Hardware Management Console (HMC) VPP Setup" of [CCGUIDE] provides detailed information on how to correctly configure the TOE in the evaluated configuration through the HMC.

The following subsections of [CCGUIDE] explain how each item will need to be adhered to in the evaluated configuration:

- 4.3.1 Password Policy - provides instruction on how to configure the password policy for the HMC.
- 4.3.2 User Creation - describes how a new user can be created;
- 4.3.3 User login and session - provides instructions on how to login as well as on any necessary preparatory steps to logging in;
- 4.3.4 Inactivity timeout configuration for HMC users - provides details on the configuration of the maximum limit of time a user can be inactive before being automatically logged off the session;
- 4.3.5 Lockout Policy configuration for HMC Users - Describes how to configure the lockout policy
- 4.3.6 Banner and Welcome Text configuration on HMC for CLI and GUI - describes how a banner can be added to both the CLI and GUI login pages;
- 4.3.7 SSH ciphers and algorithms configuration - provides instructions for configuring the TOE to use the ECC P-256 and P-384 NIST curve schemes for key establishment, and how to set up key generation using RSA, both when the HMC acts as a server and when it acts as a client;
- 4.3.8 SSH authentication methods - guides the user in setting the authentication methods to password and public key;
- 4.3.9 SSH Rekey configuration - provides instructions on how to enable the ssh rekey functionality with the required thresholds;
- 4.3.10 SSH Packet Size configuration - provides the necessary steps to configure the ssh maximum packet length;
- 4.3.11 SSH Key Based Authentication configuration - instructs the user on how to configure SSH key based authentication for when the HMC acts as a server or a client;
- 4.3.12 SSH known hosts management in local database - provides instructions on how to add public keys for a certain host name to the .ssh/known_hosts file;
- 4.3.13 CA-Signed Certificate and cyphers setting for TLS - provides instructions on how to configure the TOE to support the approved TLS encryptions;
    - 4.3.13.1 CSR file - instructs the user on how to create certificates for TLS;
    - 4.3.13.2 Apply Certificate - instructs the user on how to apply the certificate;
    - 4.3.13.3 Archive certificate - instructs the user on how to archive the certificate;

- 4.3.14 VM Configuration - provides details on creating, configuring and deleting VMs;
- 4.3.15 Guest VM Name Focus - provides an example of how CLI Terminals used by Guest VMs clearly indicate the name of the partition on top the CLI;
- 4.3.16 XNTP service Enablement on HMC - provides clear instructions are provided on how to enable the XNTP service on the HMC;
- 4.3.17 Configure Removable Media for HMC - provides clear instructions are provided on how to configure removable media;
- 4.3.18 Configure/De-configure Network for VM - provides instructions on how to configure a Virtual Network through the web GUI of the HMC;
- 4.3.19 Configure Physical Devices for VM - specifies various steps to follow in order to configure physical devices for a guest VM through the WEB GUI;
- 4.3.20 Clearing logical volumes - provides instructions on how to manually clear a logical volume before it can be assigned to another partition;
- 4.3.21 Audit Function - provides instructions on how to import and export audit log files to an SFTP server using both password and public key mechanism.

10 Annex B – Evaluated configuration

The Target of Evaluation is “IBM PowerVM FW 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9”, developed by IBM Corp. The TOE is accompanied by guidance documentation. The items listed in Table 3represent the TOE.

The TOE name and version number uniquely identify the TOE and its components, which constitute the evaluated configuration of the TOE verified by the Evaluators at the time they perform the tests and to which the evaluation results apply.

10.1 TOE operational environment

The assumptions about the operational environment in which the TOE is intended to be used are reported in section 4.2 of [ST].

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

The test systems were running IBM PowerVM FW 1060 with VIOS 4.1.1 for Server for POWER10 and HMC for POWER9 in the evaluated configuration.

All testing activities have been carried out remotely from the LVS premises having full and exclusive control on the test machine.

All test activities have been performed according to instruction provided by OCSI in the [NIS5].

11.2 Functional tests performed by the Developer

No Developer tests assessment is required by the assurance requirements described in [ST] and [VPP].

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

The Evaluators performed tests following the CEM approach to test every security function, without striving for exhaustive testing: Evaluators devised a test strategy for the tests they developed themselves.

The Evaluators performed testing remotely by connecting to the test environment using IBM hardened laptops. The Developer set up the test environment with the actual TOE model in Austin, Texas. The testing was performed between July and September 2025.

The Evaluators developed automated, partially automated and manual test procedures: The TOE claims exact conformance to the [VPP] and [MOD_SV].

The Evaluators, for each SFR declared in the [ST], have performed all tests required by the [VPP] and the selected packages ([PKG_TLS] and [PKG_SSH]) with the addition of Technical Decisions listed in [ST], section 2 "CC Conformance Claim".

11.3.2 Test result

All test cases devised by the Evaluators were run successfully and all the test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the test environment and TOE already used for the functional test activities, verifying that the TOE and the test environment were properly configured.

The Evaluators analysed the Security Target [ST], design documentation, and test results for potential vulnerabilities. In addition, the Evaluators performed a search on public sources for known or claimed potential vulnerabilities of the TOE or components of the TOE. The Evaluators also performed fuzzing penetration testing activities against PowerVM and VIOS. The Evaluators could then

conclude that the TOE is resistant to an attack potential of **Basic** in its intended operating environment. No exploitable or residual vulnerabilities have been identified.