Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 14/22

(Certification No.)

Prodotto: *(Product)* **IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware**

Sviluppato da: *(Developed by)* **IBM Corporation**

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.2)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 27 giugno 2022

Common Criteria

SOGIS IT SECURITY CERTIFIED

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware

OCSI/CERT/ATS/14/2021/RC

Version 1.0

27 June 2022

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for 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	27/06/2022

2 Table of contents

3 Acronyms

AAS	Advanced Administration System
APAR	Authorized Program Analysis Report
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSP	Flexible Service Processor
FTP	File Transfer Protocol
HCall	Hypervisor Call
HMC	Hardware Management Console
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
I/O	Input/Output
IT	Information Technology
LGP	Linea Guida Provvisoria
LPAR	Logical Partition
LVS	Laboratorio per la Valutazione della Sicurezza
MC	Management Console
NIS	Nota Informativa dello Schema
OF/RTA	Open Firmware/Run-Time Abstraction
OCSI	Organismo di Certificazione della Sicurezza Informatica
OS	Operating System

PDF	Portable Document Format
PHYP	PowerVM Hypervisor
PP	Protection Profile
RISC	Reduced Instruction Set Computer
RPA	IBM RISC System/6000 Platform Architecture
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SLIC	System Licensed Internal Code
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
vENT	Virtual Ethernet
VIOS	Virtual Input/Output System
vSCSI	Virtual Small Computer System Interface

4 References

4.1 Criteria and regulations

[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. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[NIS120] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/20 – Condizioni per l’effettuazione di test da remoto in valutazioni Common Criteria, versione 1.0, 6 aprile 2020

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

4.2 Technical documents

[ETR] Final Evaluation Technical Report “IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware”, v1, atsec information security S.r.l., 23 June 2022

[GUI] “IBM Power 3.1.3 User Guidance”, Revision 1.1, IBM Corp., 21 June 2022

[ST] “IBM PowerVM 3.1.3 with VIOS 3.1.3.10 for POWER9 and Power10 Security Target”, Version 1.0, IBM Corp., 23 June 2022

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 recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA for all declared assurance components.

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] has been ratified on 08 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 declared assurance components.

6 Statement of certification

The Target of Evaluation (TOE) is the product “IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware”, also referred to in the following as “PowerVM”, developed by IBM Corporation.

The TOE 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]. 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 v 3.1 for the assurance level EAL2, augmented with ALC_FLR.2, according to the information provided in the Security Target [ST] 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 "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware" 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 review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware
Security Target	"IBM PowerVM 3.1.3 with VIOS 3.1.3.10 for POWER9 and Power10 Security Target", Version 1.0 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security S.r.l.
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	9 December 2021
Evaluation ending date	23 June 2022

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.

7.3 Evaluated product

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

The TOE "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware" 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.

While PowerVM performs virtualization of the CPUs and memory space, VIOS performs virtualization of storage and network devices. PowerVM supports assigning individual physical storage or network devices to a partition, but it does not support sharing of physical storage and network devices between partitions.

For a detailed description of the TOE, consult sect. 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

The TOE consists of the PowerVM Hypervisor (PHYP) and VIOS. The TOE is comprised by the following security domains:

- Hypervisor domain: the Hypervisor is virtualization software. It controls and virtualizes processors, memory space, and assigns devices (e.g., storage, networking) to a set of containers called LPARs. As such, the Hypervisor uses the POWER hardware mechanisms to isolate and protect itself from the LPARs so that the Hypervisor can maintain control over the LPARs. It also uses the POWER hardware mechanisms to isolate each LPAR from one another.

- VIOS: the Hypervisor controls and virtualize processors and memory space to a set of containers called LPARs. VIOS is a special logical partition dedicated to I/O management. All the domain separation mechanisms adopted for it are applicable to the other partitions.

While not included as part of the TOE, the TOE is configured using a connected Management Console (MC) that provides access to the functions necessary to enable administrative personnel to effectively manage the allocation of resources (i.e., processors, memory, and I/O devices) to the configured partitions.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions and threats, is defined in sect. 3 and sect. 4 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 7 of the Security Target [ST]. The most significant aspects are summarized below:

- **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 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 micro-partitions) 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 MC when it is being configured. Once configured, the configured values are continuously enforced.

- *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 MC, 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 and vENT 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.

- **Identification**: 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 MC to configure and manage the TOE.

- **Security management**: all of the TOE configuration and management occurs via the interface to the MC. Administrators can configure and manage the security function policies (SFPs) used by the TOE. All functions to configure the TOE are available only through the dedicated physical MC interface. The MC allows an administrator of the TOE to create partitions and to assign CPU, memory, and I/O device resources to those partitions. Furthermore, each given resource can be assigned only to a single partition. The resulting configuration data is pushed to the TOE prior to it being placed in an operational, evaluated configuration.

- **Protection of the TSF**: the components of the TOE protect themselves using the domains provided by the Power 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.

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 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 sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All Security Functional Requirements (SFR) have been selected from CC Part 2 [CC2].

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) 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 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].

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 23 June 2022 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 24 June 2022. 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; it remains a probability (the smaller, the higher the assurance level) 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 check regularly 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 [ETR] 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 "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.2, 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 level EAL2 augmented with ALC_FLR.2.

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
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.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
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	Pass

Assurance classes and components		Verdict
Tests	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

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

Potential customers of the product “IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions described in sect. 3.2 of the Security Target [ST] are respected.

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, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([GUI]).

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

The TOE images are downloadable from the Developer's website over an HTTPS connection. The TOE software is comprised of the following images:

- PowerVM:
    - POWER9: 01VH950_092_045 (a.k.a. FW950.30)
    - Power10: 01MH1010_094_094 (a.k.a. FW1010.10)
- VIOS:
    - Virtual_IO_Server_Base_Install_3.1.3.10_Flash_092021_LCD8250308.iso

The TOE guidance is contained in the document "IBM Power 3.1.3 User Guidance v1.1" [GUI].

The most recent level of firmware is pre-installed on the server. To place an order for an IBM Power System E980 (POWER9) or E1080 (Power10) the customer needs to contact an IBM partner or an IBM reseller which will then place the order using the e-config internal tool, specifying model, number of core activations, number of memory activations, I/O adapters, software to be pre-installed and so on. The TOE delivery start after the order is entered though e-config, and the order for the server is sent to the AAS (Advanced Administration System) system. AAS is a corporate application that administratively processes hardware and software orders. AAS sends the order for the server to the hardware manufacture order fulfillment department. The machine is packaged in a sealed box. The customer number, name, and address are inside the box. A courier service picks up the machine and delivers it to the customer. A signature is required at the point of delivery.

The CC-evaluated PowerVM firmware and VIOS can be manually downloaded from the fix central servers via an HTTPS connection and secure FTP to a client and then transfer the data from their server to the HMC/FSP via a network connection (secure FTP is available). The HMC also provides an option to use secure FTP to directly transfer the firmware from the fix central servers. The guidance document [GUI] in sect. 4.3 "System firmware installation" and 4.4 "VIOS installation" provides the steps to download, check and install the PowerVM firmware and VIOS.

9.2 Identification of the TOE

After that the TOE user has obtained the hardware and the software, he can verify that the hardware and TOE software is correct by taking the following steps:

- Verify the hardware label which state the model name and check with the one stated in the Security Target [ST].

- Verify the TOE software by checking the hash code generated by the downloaded files with the hash provided in the guidance document [GUI].

- The guidance document [GUI] is delivered by IBM as a downloadable PDF file from a secure site (HTTPS). The version number is printed in the document and must match the one stated in the Security Target [ST].

9.3 Installation, initialization and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer:

- “IBM Power 3.1.3 User Guidance”, Revision 1.1 [GUI].

The document [GUI] contains references to other relevant guidance documentation providing additional detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware”, developed by IBM Corporation.

The TOE includes the software and firmware components listed in sect. 9.1.

The CC evaluated PowerVM and VIOS requires the following non-TOE hardware and software components:

- IBM Power System E980 (POWER9);
- IBM Power System E1080 (Power10);
- Open Firmware/Run-Time Abstraction (OF/RTA) for VIOS;
- Management Consoles (MCs).

The following items will need to be adhered to in the evaluated configuration:

- I/O Pools: the user must not create a storage pool, and must remove any storage pools that exist.
- Workload Management Groups: Partitions must be configured with a workload management group of none (i.e., a numbered group is not supported).
- Power Controlling: user must not allow any partition to have a power controlling partition, and must remove any power controlling partitions if they exist.
- Shared Storage Pools: user must not create a shared storage pool. This feature is supported, but not activated on a freshly installed Virtual I/O Server.
- Cache Management: user must not enable cache management. This feature is disabled on a freshly installed Virtual I/O Server.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL2, augmented with ALC_FLR.2, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

The test environment has been prepared by the Developer following the information provided in the guidance document [GUI], which includes instructions for installing PowerVM and VIOS 3.1.3.10 on both POWER9 and Power10 systems.

All PowerVM tests have been executed by the Developer on the following TOE systems:

- IBM PowerVM FW950.30 on IBM Power System E980 (POWER9);
- IBM PowerVM FW1010.10 on IBM Power System E1080 (Power10).

In each TOE system the Developer has installed and configured a VIOS partition, on which all VIOS tests have been executed.

The test environment also included the HMC for the configuration of the test cases.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer's tests suite was designed to ensure the TOE fulfills the security objectives for the TOE as described in the Security Target [ST].

This is evidenced in the test descriptions provided throughout the manual testcase guides which not only include expected test results but also verification steps, and in the reference documentation available for the Hypervisor calls (HCalls) that are employed in the automated tests.

The provided tests for PowerVM, on both POWER9 and Power10, are all automated. Automated tests are covering all the TSFIs of the PowerVM:

- SLIC HCalls;
- RPA HCalls;
- Logical Partition events calls.

Each test corresponds to a Hypervisor call using its operation code. All the Hypervisor calls are covered by Developer tests.

The provided test for VIOS are all manual. Tests are divided into two categories covering TSFIs which are:

- Virtual Ethernet and Shared Ethernet;
- Virtual SCSI.

11.2.2 Test results

The Developer provided tests results which were generated using the TOE in its evaluated configuration installed on the test systems.

The Evaluators were able to verify that the Developer testing was executed on hardware/software compliant to the specifications described in the Security Target [ST] and the guidance documentation [GUI].

The Evaluators were also able to follow and fully understand the Developer's testing approach by using the provided test documentation.

The Evaluators analyzed the Developer testing coverage and found the testing of the TSF to be extensive and covering all the TSFIs as identified in the functional specification. Finally, the Evaluators reviewed the test results provided by the Developer and found them to be consistent with the expected test results according to the test plan.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

Evaluators' testing was performed remotely at the Developer's site in Rochester from the LVS premises in Rome, Italy. All remote test activities have been carried out in accordance with the instructions provided by the Italian Certification Body in the Scheme Information Note 1/20 - Conditions for performing tests remotely in Common Criteria evaluations [NIS120].

Before initiating the testing activity, the Evaluators verified the system configuration according to the guidance documentation [GUI] and the test plan provided by the Developer, and determined that the test configuration was consistent with the configuration under evaluation as specified in the Security Target [ST].

The Evaluators chose to run all Hypervisor's automated test and all VIOS's manual tests. The Evaluators performed tests on all hardware architectures types (POWER9 and Power10) supported in the evaluation.

In addition to running all the Developer's test cases, the Evaluators devised additional tests for a subset of the TOE security functionality. Some of the tests were based on Developer's tests, with some variations to the parameters and the configuration, while two tests were specifically created by the Evaluators to broaden the covering of some SFRs with additional checks. In particular, the following security aspects were covered by Evaluators' test:

- non-bypassability of the virtual HMC;
- failure with preservation of secure state.

11.3.2 Test results

All Developer's tests were run successfully. The Evaluators verified the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators passed, i.e., all the actual test results were consistent with the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same test environment already used for the functional test activities, verifying that the test configuration was consistent with the TOE under evaluation.

The Evaluators first performed a search of public domain sources to identify potential vulnerabilities in the TOE. The Evaluators searched several databases, including Common Vulnerabilities and Exposures (CVE), Exploit Database (EDB), and IBM Security APAR Information, using carefully chosen keywords.

As a result of this search, the Evaluators found no vulnerability which are applicable to the TOE in its evaluated configuration.

The Evaluators then examined the ST, guidance documentation, functional specification, and TOE design evidence to identify possible potential vulnerabilities in the TOE.

This analysis did not reveal really obvious oversights or possible flaws. The Evaluators then focused on complex features and interfaces of the TOE, possibly being incorrectly implemented. The Evaluator chose to test specific TSFIs using fuzzing techniques to identify flaws within the TOE.

To this purpose, the Evaluators developed a kernel module driver (hFuzzer) specific for Power architecture and Linux OS which is intended to make calls to available user-side HCalls using malformed parameters. The aim of this kind of testing is verify the absence of unexpected behaviour of the target, that is the PowerVM and the VIOS partition. No errors or inconsistencies have been identified as a result of the penetration testing.

Based on the vulnerability analysis and the penetration testing results, the Evaluators could then conclude that the TOE is resistant to an attack potential of Basic in its intended operational environment. No exploitable or residual vulnerabilities have been identified.