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)

Firmato digitalmente
da Eva Spina
Data: 2022.06.27
16:05:02 +02'00'

Roma, 27 giugno 2022

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

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

Rapporto di Certificazione

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

Versione 1.0

27 giugno 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	27/06/2022

2 Indice

3 Elenco degli acronimi

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
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
ODV	Oggetto della Valutazione
OF/RTA	Open Firmware/Run-Time Abstraction
OCSI	Organismo di Certificazione della Sicurezza Informatica
PDF	Portable Document Format

PHYP	PowerVM Hypervisor
PP	Protection Profile
RFV	Rapporto Finale di Valutazione
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
TDS	Traguardo di Sicurezza
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 Riferimenti

4.1 Criteri e normative

[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 Documenti tecnici

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

[RFV] 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

[TDS] “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 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su https://www.sogis.eu/.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia dichiarati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia dichiarati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware", nel seguito del documento anche indicato come "PowerVM", sviluppato da IBM Corporation.

L'ODV facilita la condivisione di risorse hardware da parte di applicazioni diverse. L'ODV si basa sul concetto di "hypervisor", progettato per istanziare "partizioni", ciascuna con le proprie risorse distinte, che appaiono alle applicazioni in esse ospitate come una piattaforma sottostante completamente funzionale.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in .

Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware
Traguardo di Sicurezza	"IBM PowerVM 3.1.3 with VIOS 3.1.3.10 for POWER9 and Power10 Security Target", Version 1.0 [TDS]
Livello di garanzia	EAL2 con l'aggiunta di ALC_FLR.2
Fornitore	IBM Corporation
Committente	IBM Corporation
LVS	atsec information security S.r.l.
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	9 dicembre 2021
Data di fine della valutazione	23 giugno 2022

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware" facilita la condivisione di risorse

hardware da parte di applicazioni diverse (ad es., AIX, IBM I, Linux). L'ODV si basa sul concetto di "hypervisor", progettato per istanziare "partizioni", ciascuna con le proprie risorse distinte, che appaiono alle applicazioni in esse ospitate come una piattaforma sottostante completamente funzionale. L'ODV è progettato per prevenire interferenze tra queste partizioni, chiamate partizioni logiche (LPAR), e per impedire la condivisione simultanea dello spazio di archiviazione e delle altre risorse del dispositivo. VIOS consente alle partizioni, mediante controllo di accesso, la condivisione di singoli dispositivi di archiviazione e di rete. L'ODV è indifferente all'applicazione in esecuzione in una LPAR.

PowerVM si occupa della virtualizzazione delle CPU e dello spazio di memoria, mentre VIOS esegue la virtualizzazione dei dispositivi di archiviazione e di rete. PowerVM supporta l'assegnazione a una partizione di singoli dispositivi fisici di archiviazione o di rete, ma non supporta la condivisione di tali dispositivi fisici tra diverse partizioni.

Per una descrizione dettagliata dell'ODV, si consulti il par. 1.4 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

L'ODV è costituito da PowerVM Hypervisor (PHYP) e da VIOS. L'ODV comprende i seguenti domini di sicurezza:

- Dominio dell'Hypervisor: l'Hypervisor è un software di virtualizzazione che controlla e virtualizza processori e spazio di memoria e assegna dispositivi (ad es., di memoria o di rete) a una serie di contenitori chiamati LPAR. L'Hypervisor utilizza i meccanismi hardware dei sistemi POWER per isolarsi e proteggersi dalle LPAR, in modo da mantenere il controllo su di esse. L'Hypervisor utilizza gli stessi meccanismi hardware per isolare ogni LPAR dalle altre.

- VIOS: l'Hypervisor controlla e virtualizza i processori e lo spazio di memoria in un insieme di contenitori chiamati LPAR. VIOS è una partizione logica speciale dedicata alla gestione dell'I/O. Tutti i meccanismi di separazione dei domini adottati per esso sono applicabili alle altre partizioni.

L'ODV viene configurato mediante una Management Console (MC) ad esso connessa che fornisce l'accesso alle funzioni necessarie per consentire agli amministratori di gestire efficacemente l'allocazione delle risorse (ad esempio, processori, memoria e dispositivi di I/O) alle partizioni configurate. La MC non fa parte dell'ODV.

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi e minacce, è definito nel cap. 3 e nel cap. 4 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 7 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Protezione dei dati d'utente**:

    - *Hypervisor*: l'Hypervisor gestisce l'associazione di CPU, memoria e dispositivi di I/O, in un ambiente relativamente statico, con partizioni contenenti istanze del sistema operativo. I dispositivi di memorizzazione e di

I/O possono essere assegnati a singole partizioni e in questo caso sono accessibili solo da quelle partizioni (inclusi OF/RTA e il sistema operativo in esecuzione nella partizione). Le CPU possono anche essere assegnate a una singola partizione e solo quella partizione (e occasionalmente l'ODV) può utilizzare quella CPU. Le CPU possono anche essere configurate per essere condivise tra un insieme di partizioni (partizioni del processore condivise, chiamate anche micropartizioni); l'Hypervisor salva e ripristina lo stato del registro hardware quando si passa da una partizione all'altra. Le partizioni non hanno alcun controllo sulle risorse che vengono loro assegnate. L'Hypervisor riceve le informazioni sulla gestione della partizione dall'MC durante la configurazione. Una volta configurati, i valori delle impostazioni vengono applicati in maniera continua.

  - *VIOS*: VIOS gestisce l'associazione di partizioni a dispositivi di archiviazione e di rete virtualizzati e l'associazione di dispositivi di archiviazione e di rete virtualizzati a dispositivi di archiviazione e di rete fisici. Tramite l'MC, un amministratore assegna un insieme di dispositivi di archiviazione e di rete fisici alla partizione VIOS. L'amministratore crea quindi dispositivi virtuali di archiviazione (vSCSI) e di rete (vENT) in VIOS, associa i dispositivi fisici ai dispositivi virtualizzati e associa questi ultimi ad altre partizioni del sistema. Queste altre partizioni accedono all'archiviazione e alla rete virtualizzati controllati da VIOS. VIOS garantisce la separazione tra i vari dispositivi virtuali di archiviazione e di rete, in modo che una partizione non possa accedere alle informazioni di un'altra partizione.

- **Identificazione**: le partizioni vengono identificate implicitamente da identificatori numerici interni associati alle partizioni (utilizzando strutture di dati interne) quando vengono definite. Essendo implicitamente identificate dall'ODV, le partizioni non hanno la necessità, né la possibilità, di identificarsi. Inoltre, l'identificazione di una partizione è garantita dall'Hypervisor. L'Hypervisor identifica gli amministratori autorizzati alla configurazione e alla gestione delle partizioni e dei dispositivi VIOS. Gli amministratori utilizzano l'MC per configurare e gestire l'ODV.

- **Gestione della sicurezza**: tutta le operazioni di configurazione e gestione dell'ODV avvengono tramite l'interfaccia verso la MC. Gli amministratori possono configurare e gestire le policy delle funzioni di sicurezza (SFP) utilizzate dall'ODV. Tutte le funzioni per configurare l'ODV sono disponibili unicamente tramite l'interfaccia fisica dedicata della MC. L'MC consente a un amministratore dell'ODV di creare partizioni e di assegnare risorse di CPU, memoria e dispositivi di I/O a tali partizioni. Inoltre, ogni specifica risorsa può essere assegnata solo a una singola partizione. I dati di configurazione risultanti vengono inviati all'ODV prima che questo venga posto nella configurazione operativa valutata.

- **Protezione del TSF**: i componenti dell'ODV proteggono sé stessi utilizzando i domini forniti dai processori Power. L'Hypervisor opera nel dominio privilegiato e le partizioni, come VIOS, operano nel dominio senza privilegi. Ciò consente all'Hypervisor di proteggere sé stesso e le risorse che mette selettivamente a disposizione delle varie partizioni. Oltre a proteggere sé stesso e le sue risorse, l'ODV è progettato in modo tale che quando l'hardware che supporta una partizione si guasta, le altre partizioni continuano ad operare senza interruzioni.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS atsec information security S.r.l.

L'attività di valutazione è terminata in data 23 giugno 2022 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 24 giugno 2022. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in .

Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS atsec information security S.r.l. e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in .

Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Security-enforcing functional specification	ADV_FSP.2	Positivo
Basic design	ADV_TDS.1	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Use of a CM system	ALC_CMC.2	Positivo
Parts of the TOE CM coverage	ALC_CMS.2	Positivo
Delivery procedures	ALC_DEL.1	Positivo

Classi e componenti di garanzia		Verdetto
Flaw reporting procedures	*ALC_FLR.2*	Positivo
Test	**Classe ATE**	Positivo
Evidence of coverage	ATE_COV.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability analysis	AVA_VAN.2	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 5.1 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le ipotesi descritte nel par. 3.2 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella sua configurazione valutata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'inizializzazione, all'installazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([GUI]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

Le immagini dell'ODV sono scaricabili dal sito Web del Fornitore tramite una connessione HTTPS. Il software dell'ODV è composto dalle seguenti immagini:

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

La documentazione di guida dell'ODV consiste nel documento "IBM Power 3.1.3 User Guidance v1.1" [GUI].

Il livello di firmware più recente è preinstallato sul server. Per effettuare un ordine per un server IBM Power System E980 (POWER9) o E1080 (Power10) il cliente deve contattare un partner IBM o un rivenditore IBM che poi effettuerà l'ordine utilizzando lo strumento interno e-config, specificando modello, numero di attivazioni di *core*, numero di attivazioni di memoria, adattatori I/O, software da preinstallare e così via. La fase di consegna dell'ODV inizia dopo che l'ordine è stato inserito tramite e-config e l'ordine per il server viene inviato al sistema AAS (Advanced Administration System). AAS è un'applicazione aziendale che elabora amministrativamente gli ordini di hardware e software. AAS invia l'ordine per il server al reparto di evasione degli ordini della produzione hardware. La macchina viene imballata in una scatola sigillata. Il numero, il nome e l'indirizzo del cliente sono all'interno della scatola. Un corriere preleva la macchina e la consegna al cliente. È necessaria una firma al punto di consegna.

Il firmware PowerVM e il sistema VIOS valutati CC possono essere scaricati manualmente su un client dai server centrali di aggiornamento tramite una connessione HTTPS e FTP sicuro, e quindi trasferiti dal loro server all'HMC/FSP tramite una connessione di rete (è disponibile l'FTP sicuro). L'HMC fornisce anche un'opzione per utilizzare l'FTP sicuro per trasferire direttamente il firmware dai server centrali di aggiornamento. I passaggi per scaricare, verificare e installare il firmware PowerVM e VIOS sono contenuti nel par. 4.3 ("System firmware installation") e nel par. 4.4 ("VIOS installation") del documento di guida [GUI].

9.2 Identificazione dell'ODV

Successivamente alla consegna dell'hardware e del software, l'utente dell'ODV può verificare la loro correttezza eseguendo i seguenti passaggi:

- Verifica che il nome del modello riportato sull'etichetta dell'hardware corrisponda con quello indicato nel Traguardo di Sicurezza [TDS].

- Verifica del software dell'ODV mediante confronto tra i valori *hash* generati per i file scaricati con quelli forniti nella documentazione di guida [GUI].

- La documentazione di guida [GUI] viene fornita da IBM come file PDF scaricabile da un sito protetto (HTTPS). Il numero di versione è stampato nel documento e deve corrispondere a quello indicato nel Traguardo di Sicurezza [TDS].

9.3 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente:

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

Il documento [GUI] contiene riferimenti ad altra documentazione di guida pertinente che fornisce informazioni dettagliate aggiuntive per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS].

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware", sviluppato dalla società IBM Corporation.

L'ODV comprende i componenti software e firmware elencati nel par. 9.1.

La configurazione valutata CC di PowerVM and VIOS richiede i seguenti componenti hardware e software non-ODV:

- IBM Power System E980 (POWER9);
- IBM Power System E1080 (Power10);
- Open Firmware/Run-Time Abstraction (OF/RTA) per VIOS;
- Management Console (MC).

Nella configurazione valutata devono essere rispettate le seguenti limitazioni:

- *I/O Pools*: l'utente non deve creare uno *storage pool* e deve rimuovere tutti gli *storage pool* esistenti.
- *Workload Management Groups*: le partizioni devono essere configurate con un gruppo di gestione del carico di lavoro pari a "nessuno" (ovvero, un gruppo numerato non è supportato).
- *Power Controlling*: l'utente non deve consentire a nessuna partizione di avere una partizione di controllo dell'alimentazione e deve rimuovere eventuali partizioni di controllo dell'alimentazione, se esistenti.
- *Shared Storage Pools*: l'utente non deve creare uno *storage pool* condiviso. Questa funzione è supportata, ma non attivata su un Virtual I/O Server appena installato.
- *Cache Management*: l'utente non deve abilitare la gestione della cache. Questa funzione è disabilitata su un Virtual I/O Server appena installato.

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, tali attività tali attività prevedono tre passi successivi:

- valutazione dei test eseguiti dal Fornitore in termini di copertura;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

L'ambiente di test è stato preparato dal Fornitore seguendo le indicazioni fornite nella documentazione di guida [GUI], che include le istruzioni per l'installazione di PowerVM e VIOS 3.1.3.10 su entrambi i sistemi POWER9 e Power10.

Tutti i test di PowerVM sono stati eseguiti dal Fornitore sui seguenti sistemi dell'ODV:

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

L'ambiente di test include anche una HMC per la configurazione dei casi di test.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

La suite di test del Fornitore è stata progettata per garantire che l'ODV soddisfi gli obiettivi di sicurezza per l'ODV descritti nel Traguardo di Sicurezza [TDS].

Ciò è evidenziato nelle descrizioni dei test fornite nelle guide dei casi di test manuali, che non includono solo i risultati previsti dei test, ma anche le fasi di verifica, e nella documentazione di riferimento disponibile per le chiamate dell'Hypervisor (HCalls) utilizzate nei test automatizzati.

I test predisposti per PowerVM, su POWER9 e su Power10, sono tutti automatizzati. I test automatizzati coprono tutte le TSFI di PowerVM:

- SLIC HCalls;
- RPA HCalls;
- Chiamate per i *Logical Partition events*.

Ogni test corrisponde a una chiamata dell'Hypervisor mediante il relativo codice operativo. I test del Fornitore coprono tutte le chiamate dell'Hypervisor.

I test predisposti per VIOS sono tutti manuali. I test sono divisi in due categorie che coprono le TSFI relative a:

- Virtual Ethernet e Shared Ethernet;
- Virtual SCSI.

11.2.2 Risultati dei test

Il Fornitore ha messo a disposizione i risultati dei test generati utilizzando l'ODV nella sua configurazione valutata installata sui sistemi di test.

I Valutatori hanno potuto verificare che i test del Fornitore sono stati eseguiti su hardware e software conformi a quanto specificato nel Traguardo di Sicurezza [TDS] e nella documentazione di guida [GUI].

I Valutatori sono stati altresì in grado di seguire e comprendere appieno l'approccio del Fornitore ai test utilizzando la documentazione di test fornita.

I Valutatori hanno analizzato la copertura dei test del Fornitore e hanno riscontrato che il TSF è stato testato in maniera estesa e che tutte le TSFI identificate nelle specifiche funzionali sono state coperte. Infine, i Valutatori hanno esaminato i risultati dei test del Fornitore e li hanno trovati conformi con i risultati previsti secondo il piano di test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

11.3.1 Approccio adottato per i test

I test dei Valutatori sono stati eseguiti presso la sede del Fornitore a Rochester, Stati Uniti, operando da remoto dalla sede di Roma dell'LVS. Tutte le attività di test in modalità remota sono state svolte in conformità alle indicazioni fornite dall'Organismo di Certificazione nella Nota Informativa dello Schema 1/20 - Condizioni per l'effettuazione di test da remoto in valutazioni Common Criteria [NIS120].

Prima di iniziare l'attività di test, i Valutatori hanno verificato la configurazione del sistema in base alla documentazione di guida [GUI] e al piano di test del Fornitore, e hanno determinato che la configurazione dell'ambiente di test era coerente con la configurazione in valutazione, come specificato nel Traguardo di Sicurezza [TDS].

I Valutatori hanno scelto di eseguire tutti i test automatici dell'Hypervisor e tutti i test manuali di VIOS. I valutatori hanno eseguito i test su tutti i tipi di architetture hardware (POWER9 e Power10) supportate nella valutazione.

In aggiunta all'esecuzione di tutti i casi di test del Fornitore, i Valutatori hanno ideato test aggiuntivi per un sottoinsieme della funzionalità di sicurezza dell'ODV. Alcuni dei test sono stati derivati dai test del Fornitore, con alcune variazioni ai parametri e alla configurazione, mentre due test sono stati creati appositamente dai Valutatori per ampliare la copertura di alcuni SFR con verifiche aggiuntive. In particolare, i seguenti aspetti di sicurezza sono stati oggetto dei test dei Valutatori:

- non aggirabilità dell'HMC virtuale;

- conservazione dello stato sicuro a seguito di guasto.

11.3.2 Risultati dei test

Tutti i test del Fornitore sono stati eseguiti con successo. I Valutatori hanno verificato il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

Tutti i casi di test progettati dai Valutatori hanno avuto esito positivo, ovvero tutti i risultati dei test sono risultati conformi a quelli previsti.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività i Valutatori hanno lavorato sullo stesso ambiente di test già utilizzato per le attività dei test funzionali, verificando che la configurazione di test fosse congruente con la versione dell'ODV in valutazione.

In una prima fase, i Valutatori hanno condotto ricerche su fonti pubbliche per identificare potenziali vulnerabilità dell'ODV. I Valutatori hanno eseguito ricerche in diversi database, tra cui Common Vulnerabilities and Exposures (CVE), Exploit Database (EDB) e IBM Security APAR Information, utilizzando parole chiave accuratamente selezionate.

Come risultato di questa attività, i Valutatori non hanno riscontrato alcuna vulnerabilità applicabile all'ODV nella sua configurazione valutata.

I Valutatori hanno quindi condotto una ricerca sulle evidenze di valutazione, inclusi TDS, documentazione di guida, specifiche funzionali e progettazione dell'ODV al fine di identificare potenziali vulnerabilità dell'ODV.

Questa analisi non ha rivelato errori evidenti o possibili difetti. I Valutatori si sono quindi concentrati su funzionalità e interfacce complesse dell'ODV, che potrebbero essere state implementate in modo errato. I Valutatori hanno scelto di testare specifiche TSFI utilizzando tecniche di *fuzzing* per identificare difetti all'interno dell'ODV.

A tale scopo, i Valutatori hanno sviluppato un modulo driver del *kernel* (hFuzzer), specifico per l'architettura Power e per il sistema operativo Linux, che effettua chiamate alle HCall disponibili lato utente utilizzando parametri malformati. Lo scopo di questo tipo di test è verificare l'assenza di comportamenti imprevisti dell'oggetto analizzato, ossia PowerVM e la partizione VIOS. I test di intrusione non hanno evidenziato errori o anomalie.

Sulla base dell'analisi di vulnerabilità e dei risultati dei test di intrusione, i Valutatori hanno stabilito che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state identificate vulnerabilità sfruttabili o residue.