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. 3/21

(Certification No.)

Prodotto: HCL BigFix version 10.0.1.41

(Product)

Sviluppato da: HCL Technologies Limited

(Developed by)

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

Il Direttore
(Dott.ssa Eva Spina)

Roma, 6 maggio 2021

Firmato digitalmente
da Eva Spina
Data: 2021.05.06
10:14:17 +02'00'

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

HCL BigFix version 10.0.1.41

OCSI/CERT/ATS/07/2020/RC

Versione 1.0

6 maggio 2021

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	06/05/2021

2 Indice

3 Elenco degli acronimi

API	Application Programming Interface
BES	BigFix Enterprise Suite
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CPU	Central Processing Unit
DNS	Domain Name System
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GB	GigaByte
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
HW	Hardware
IEM	IBM Endpoint Manager
ISO/OSI	International Organization for Standardization / Open Systems Interconnection
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PC	Personal Computer
PGP	Pretty Good Privacy
PP	Profilo di Protezione (Protection Profile)

RAM	Random Access Memory
REST	Representational State Transfer
RFV	Rapporto Finale di Valutazione
RHEL	Red Hat Enterprise Linux
RPM	Red Hat Package Manager
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
SO	Sistema Operativo
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
ST	Security Target
SW	Software
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Fanctionality
TLS	Transport Layer Security
UDP	User Datagram Protocol
XML	eXtensible Markup Language

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

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

4.2 Documenti tecnici

[BFASG] BigFix Version 10.0.1 Action Script Guide

[BFCCCG] HCL BigFix Version 10.0.1 Common Criteria Configuration Guide, Version 1.9, 26 October 2021

[BFCG] BigFix Configuration Guide, Version 10.0

[BFCO] BigFix Console Operator's Guide, Version 10.0

[BFIG] BigFix Installation Guide, Version 10.0

[BFRA] BigFix Version 10.0.1 REST API

[BFRG] BigFix Version 10.0.1 Relevance Guide

[RFV] Final Evaluation Technical Report "HCL BigFix version 10.0.1.41", OCSI-CERT-ATS-07-2020_ETR_210322_v1.1, Version 1.1, atsec information security GmbH, 22 March 2021

[TDS] HCL BigFix version 10.0.1 Common Criteria Security Target, Version 1.4, HCL Technologies Limited, 26 February 2021

5 Riconoscimento del certificato

5.1 Riconoscimento dei 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 fino al livello di garanzia EAL2.

5.2 Riconoscimento dei 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 fino al livello di garanzia EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto software "HCL BigFix version 10.0.1.41", nel seguito del documento anche indicato come "HCL BigFix", sviluppato da HCL Technologies Limited.

L'ODV è un sistema di gestione centralizzato degli endpoint che consente agli operatori autorizzati di monitorare le configurazioni di sistema degli endpoint distribuiti (computer client) e consente agli operatori di effettuare tutte le azioni correttive necessarie.

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, 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 "HCL BigFix version 10.0.1.41" 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 previsto.

7.2 Identificazione sintetica della valutazione

Nome dell'ODV	HCL BigFix version 10.0.1.41
Traguardo di sicurezza	HCL BigFix version 10.0.1.41 Common Criteria Security Target, Version 1.4 [TDS]
Livello di garanzia	EAL2
Fornitore	HCL Technologies Limited
Committente	HCL Technologies Limited
LVS	atsec information security Srl
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	4 agosto 2020
Data di fine della valutazione	22 marzo 2021

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 è un'applicazione client-server che consente il monitoraggio e la gestione di sistemi IT raggiungibili da una posizione centrale. L'ODV utilizza una tecnologia Fixlet® brevettata per identificare i computer vulnerabili o mal configurati nell'azienda e consente agli utenti autorizzati di correggere i problemi identificati in rete.

I messaggi Fixlet sono disponibili per un'azienda registrandosi ad uno qualsiasi dei diversi siti Fixlet gestiti dal BigFix Fixlet Server che non fa parte dell'ODV ed è al di fuori della configurazione valutata. Ogni sito Fixlet contiene messaggi Fixlet preconfigurati e testati che forniscono soluzioni di gestione pronte all'uso. Questi costituiscono dati che l'ODV raccoglie, distribuisce e utilizza in altro modo tramite Internet dal BigFix Fixlet Server per rilevare e correggere le vulnerabilità.

I Fixlet consentono agli utenti autorizzati di eseguire le seguenti funzioni all'interno dell'azienda:

- analizzare lo stato di vulnerabilità (ovvero, configurazioni con patch o non sicure);
- distribuire le patch ai computer vulnerabili per mantenere la sicurezza degli endpoint;
- stabilire e applicare le politiche di sicurezza della configurazione attraverso la rete;
- distribuire e aggiornare il software;
- gestire la rete da una Console centrale;
- visualizzare, modificare e controllare le proprietà e le configurazioni dei computer client in rete.

L'ODV contiene al suo interno funzionalità crittografiche con chiave pubblica/privata per garantire l'autenticità dei messaggi Fixlet e delle azioni correttive. Ogni Fixlet e Action ricevuti da un BigFix Client viene autenticato verificando una firma digitale apposta dall'amministratore di riferimento per garantire che sia stata generata da un amministratore autorizzato a eseguire le operazioni corrispondenti. Queste operazioni autorizzate istruiscono i BigFix Client a visualizzare, modificare e controllare le proprietà e le configurazioni dei computer client in rete. I risultati di tali operazioni, o semplicemente i dati raccolti, vengono cifrati e restituiti al server BES.

7.3.1 Architettura dell'ODV

L'ODV consiste in quattro component software:

- BigFix Server
- BigFix Console
- BigFix Client (o Agent)
- BigFix Relay

Durante l'installazione dell'ODV, l'amministratore autorizzato del sito crea un Masthead che lega insieme gli elementi dell'ODV. Tra le altre cose, il Masthead include una chiave (firmata dall'amministratore del sito) per autenticare le istruzioni ricevute dal BigFix Server. Di seguito è riportata una panoramica di ciascuno dei componenti, denominati per brevità Server, Console, Client e Relay.

L'ODV fornisce a un utente autorizzato la capacità di valutare lo stato del Sistema Operativo (SO) delle macchine client, delle applicazioni, delle firme antivirus, ecc. (mediante le Fixlet) e offre la possibilità di aggiornare queste macchine secondo necessità (mediante le Azioni). L'ODV si basa sulla capacità delle macchine client di verificare periodicamente con il server (o il relay designato) le Fixlet e/o le Azioni più recenti che si possono ottenere.

La Figura 1 mostra una panoramica dell'architettura di base dell'ODV. È presente almeno un server che raccoglie Fixlet dal BigFix Server su Internet dove possono essere visualizzati dall'operatore della console e distribuiti ai relay. Ogni client ispeziona il proprio ambiente informatico locale e segnala eventuali Fixlet pertinenti al relay, che comprime i dati e li ritrasmette ai server.

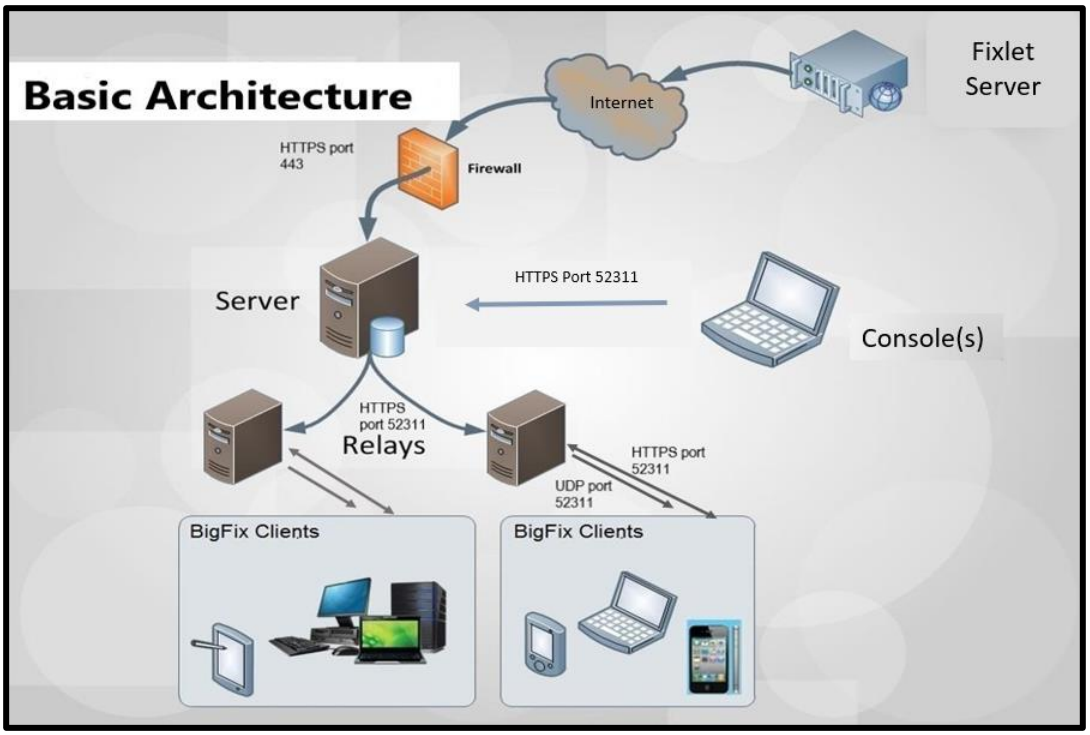

Figura 1 - Archiettura dell'ODV

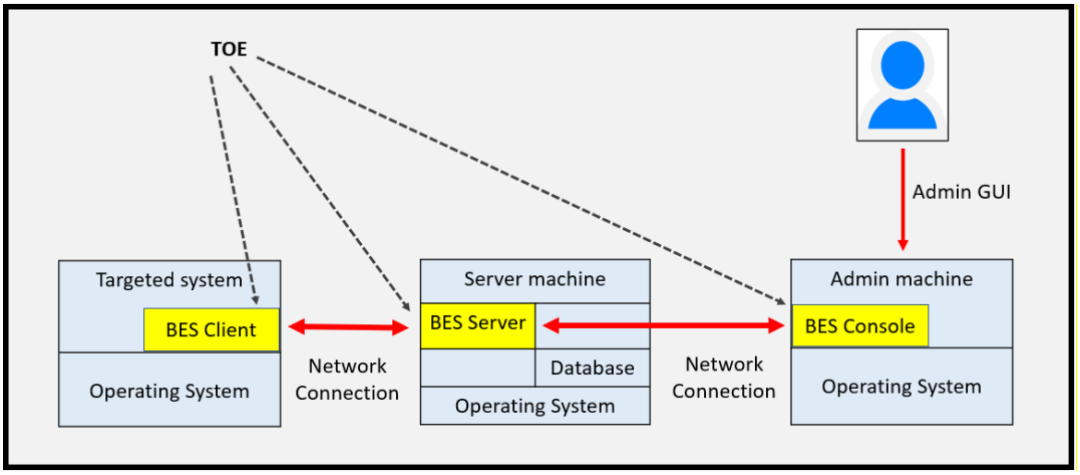

Figura 2 - Rappresentazione logica dell'ODV

Le frecce piene nella Figura 1 individuano i componenti dell'ODV richiesti nonché il servizio Fixlet opzionale nell'ambiente IT fornito da BigFix tramite Internet. Si noti che nonostante la Figura 1 rappresenti l'ODV come un insieme di computer di vario tipo, l'ODV è costituito solo da software in esecuzione nel contesto dei computer e dei sistemi operativi installati su di essi.

La Figura 2 fornisce una rappresentazione logica dei componenti principali dell'ODV nel contesto dei computer in cui è installato. Si noti che un Relay è essenzialmente una combinazione di componenti client e server che agiscono per archiviare e inoltrare le comunicazioni in entrambe le direzioni. I Relay sono componenti opzionali che non influenzano le funzioni di sicurezza dell'ODV, ma incrementano l'efficienza della rete nella distribuzione di Fixlet e Azioni.

7.3.2 Caratteristiche di sicurezza dell'ODV

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

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il par. 1.4.3 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Supporto crittografico**: l'ODV esegue operazioni crittografiche fornendo coppie di chiavi pubbliche/private Rivest-Shamir-Adleman (RSA) allo scopo di firmare digitalmente le Azioni all'interno dell'infrastruttura. Queste firme consentono all'ODV di autenticare e garantire lintegrità delle azioni correttive mentre vengono raccolte, distribuite e implementate da vari componenti dell'ODV in rete. Per proteggere i dati raccolti dai Client, l'ODV genera coppie di chiavi pubbliche/private RSA utilizzate per la crittografia che vengono distribuite dal server ai Client e ai Relay.

- **Protezione dei dati dell'utente**: l'ODV fornisce una Action Information Flow Control SFP che controlla l'applicazione delle Azioni tramite i Client. Le Azioni sono fornite dagli Operatori. Il server dell'ODV facilita la distribuzione delle Azioni applicabili ai Client e tali Client accettano e applicano le Azioni solo quando può essere verificato che provengono da una fonte autorizzata (ad esempio, un Operatore assegnato alla gestione dello specifico Client).

- **Identificazione e autenticazione (I&A)**: l'ODV richiede che gli utenti (ovvero gli amministratori) siano identificati e autenticati prima di effettuare qualsiasi azione relativa alla gestione della sicurezza. Una volta che un amministratore è stato autenticato, l'ODV impone regole basate sui ruoli assegnati e solo il Master Operator può modificare le regole e gli attributi per conto degli utenti.

- **Gestione della sicurezza**: l'ODV fornisce funzioni di gestione della sicurezza a cui possono accedere solo gli amministratori autorizzati. L'ODV limita la capacità di determinare il comportamento, disabilitare, abilitare, modificare il comportamento delle funzioni (ovvero, regole e privilegi della politica di sicurezza) in base al ruolo e fornisce anche le funzioni necessarie per una gestione efficace delle funzioni di sicurezza dell'ODV.

- **Protezione delle funzioni di sicurezza dell'ODV (TSF)**: l'ODV impone l'uso di TLS v1.2/HTTPS per proteggere il canale di comunicazione tra tutti i componenti dell'ODV (Server, Console, Relay e Client). L'ODV protegge la sicurezza dei dati e dei risultati delle operazioni che vengono raccolti sui computer client in rete cifrando questi dati prima che vengano trasmessi sulla rete.

- **Percorsi/canali fidati**: l'ODV impone l'uso di TLS v1.2/HTTPS per proteggere il canale di comunicazione tra l'ODV ed i Fixlet Server, che sono considerati entità IT esterne. L'ODV impone l'uso di TLS v1.2 per l'interfaccia API REST fornita dall'ODV per consentire a entità IT esterne di eseguire funzioni di gestione della sicurezza.

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 (SFR) sono stati derivati dai CC Parte 2 [CC2].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (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 Srl.

L'attività di valutazione è terminata in data 22 marzo 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 26 marzo 2021. 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 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 "HCL BigFix version 10.0.1.41" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, 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.

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
Tests	**Classe ATE**	Positivo
Evidence of coverage	ATE_COV.1	Positivo
Functional testing	ATE_FUN.1	Positivo

Classi e componenti di garanzia		Verdetto
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 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "HCL BigFix version 10.0.1.41" 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 e le Politiche di sicurezza organizzative descritte rispettivamente nel par. 3.2 e nel par. 3.3 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, in particolare in Appendice A – Indicazioni per l'uso sicuro del prodotto sono incluse alcune raccomandazioni relative alla consegna, all'inzializzazione e e utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([BFASG], [BFCCCG], [BFCG], [BFCM], [BFCO], [BFIG], [BFRA], [BFRG]).

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

La procedura di consegna dell'ODV consiste nello scaricamento e nella verifica dei seguenti file dal BigFix Enterprise Suite Download Center:

- BigFix Installation Generator
- Hot fix version 10.0.1.45 for BigFix Administration tool
- BigFix Clients
- BigFix Guidance

La versione valutata di HCL BigFix 10.0.1.41 è disponibile come file autoestraente (.exe). In particolare, l'immagine del server BigFix Windows, chiamata Installation Generator - Windows (BigFix 10.0.1.41.exe), contiene il server HCL BigFix, il Client HCL BigFix, la Console HCL BigFix ed il BigFix Administration Tool.

L'eseguibile dell'hot fix per il BigFix Administration Tool è attualmente disponibile all'indirizzo: https://software.bigfix.com/download/bes/100/10.0.1.45/BESAdmin.exe.

L'ODV include anche due Client BigFix disponibili per Windows 10 e per le piattaforme RHEL 6-8. In particolare, l'immagine del BigFix Client per Windows è disponibile nella cartella di installazione del BigFix Server, mentre l'immagine del BigFix Client per RHEL può essere scaricata dal Download Center.

Prima di utilizzare l'ODV, è necessario verificare i file scaricati nel modo seguente:

- *Pacchetti Windows*: per garantire l'autenticità del software scaricato, i file Windows sono firmati digitalmente da "HCL America Inc.". Le informazioni sull'integrità sono disponibili per ogni pacchetto in termini di dimensione, firma SHA-1, firma SHA-256, semplicemente aprendo le proprietà del file su Windows.

- *Pacchetti RPM*: per garantire l'autenticità dei pacchetti RPM di Red Hat, questi sono firmati con una chiave PGP. I file sono firmati digitalmente da "IBM Corp. and HCL Technologies Limited". È possibile scaricare e importare la chiave pubblica corrispondente a questa firma eseguendo la BES Support Fixlet denominata Import BigFix version 9.5 public GPG key for RedHat RPMs. Per ulteriori informazioni su come importare la chiave PGP e verificare il pacchetto consultare il capitolo "Signed Client Red Hat RPM packages" della documentazione PDF "BigFix Installation Guide" [BFIG].

- *Guide*: per garantire l'autenticità dei file scaricati, sono disponibili informazioni sull'integrità per ciascuna guida in termini di dimensione, firma SHA-1, firma SHA-256.

L’ODV viene attivato da una chiave di licenza. Le informazioni sulle chiavi di licenza possono essere ottenute dal team HCL Federal Sales Operations o dall’HCL Federal Support Center for information.

9.2 Installazione, initializzazione e utilizzo sicuro dell’ODV

Per l’installazione e la configurazione sicura dell’ODV fare riferimento ai documenti di guida [BFIG], [BFCG] e [BFCCCG], dove viene fornita la configurazione della piattaforma BigFix insieme ad alcuni esempi di scenari di distribuzione, scenari di configurazione e tipi di installazione su macchine Windows e Linux. Sono incluse anche le attività di gestione della piattaforma. In [BFCCCG] vengono forniti i dettagli su come applicare l'hot fix.

Per un utilizzo sicuro dell’ODV fare riferimento ai documenti di guida [BFASG], [BFCO], [BFRA] e [BFRG] che contengono informazioni sull’utilizzo della Console, delle API REST, degli script e del Relevance language.

10 Appendice B – Configurazione valutata

La configurazione valutata è costituita dal software e dalla documentazione di guida specificata nella sezione 1.4.2 del Traguardo di Sicurezza [TDS]. In particolare, i componenti SW dell'ODV sono i seguenti:

- BigFix Server 10.0.1.41
- BigFix Client 10.0.1.41
- BigFix Relay 10.0.1.41
- BigFix Console 10.0.1.41
- BigFix Administration Tool 10.0.1.45

La documentazione guida è costituita dai seguenti documenti: [BFASG], [BFCCCG], [BFCG], [BFCM], [BFCO], [BFIG], [BFRA], [BFRG].

Gli scenari di distribuzione degli elementi HW e SW includono una configurazione minima in cui è disponibile almeno un componente per HCL BigFix Server, HCL BigFix Client, HCL BigFix Console e HCL BigFix Administration Tool. La Tabella 2 mostra la configurazione minima dell'ODV e i componenti aggiuntivi opzionali.

Componente SW	Numero di componenti installati	Sistema operative della macchina host
HCL BigFix Server	uno	Windows Server 2016
HCL BigFix Client	uno	Windows Server 2016
HCL BigFix Console	uno	Windows Server 2016
HCL BigFix Administration Tool	uno	Windows Server 2016
HCLBigFixRelay	nessuno o più	Windows 10
HCL BigFix Client	nessuno o più	Windows 10
HCL BigFix Client	nessuno o più	RHEL 7
HCL BigFix Console	nessuno o più	Windows Server 2016
HCL BigFix Client	nessuno o più	Windows Server 2016

Tabella 2 – Scenari di distribuzione dell'ODV

Ogni componente dell'ODV richiede hardware e software aggiuntivi che costituiscono l'ambiente operativo. Il software e l'hardware richiesti da ciascun componente dell'ODV sono elencati di seguito:

- BigFix Server: Windows Server 2016, MSSQL Server 2016, Processore X86-64 (4CPU), RAM da 16 GB, Disco da 250 GB

- BigFix Console: Windows Server 2016, Processore X86-64 (2CPU), RAM da 4 GB RAM, Disco da 20 GB
- BigFix Relay: Windows 10, Processore X86-64 (2CPU), RAM da 4 GB, Disco da 25 GB
- BigFix Client: Sistemi operativi supportati (Windows Server 2016, Windows 10, Red Hat Enterprise Linux 7), Processore X86-64 (2CPU), RAM da 4 GB, Disco da 20 GB

Per l'ODV è necessario anche il database MSSQL 2016 che fa anch'esso parte dell'ambiente operativo. L'installazione e la configurazione di MSSQL 2016 è un prerequisito per il componente server dell'ODV.

L'ODV richiede anche il servizio Domain Name System (DNS) nell'ambiente operativo.

Alla configurazione valutata si applicano le seguenti restrizioni:

- il componente Server deve essere configurato come server di autenticazione;
- il componente Server deve essere configurato per l'utilizzo di HTTPS per connettersi a siti esterni;
- il componente Server deve essere configurato per richiedere TLS v1.2 per tutte le comunicazioni HTTPS;
- il componente Server deve essere configurato per l'utilizzo di "Enhanced security".
- il componente Server deve essere configurato per l'utilizzo di "FIPS mode".
- i componenti Relay devono essere configurati come relay di autenticazione;
- i componenti Client devono essere configurati per l'invio di soli "encrypted report";
- ogni account di utente può avere un solo ruolo ad esso assegnato;
- FTP deve essere disabilitato;
- SSH deve essere disabilitato;
- l'interfaccia Web Reports deve essere disabilitata o non installata;
- l'interfaccia WebUI non deve essere installata.

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, 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

Sono stati usati i seguenti elementi software che sotituscono il pacchetto di installazione per l'ODV:

- 1 pacchetto di installazione HCL BigFix (BigFix-BES-10.0.1.41.exe)
- 1 pacchetto HCL BigFix Red Hat Client (BESAgent-10.0.1.41.rhe6.x86_64.rpm)
- 1 file da cui è stata generate una licenza (LicenseAuthorization.BESLicenseAuthorization)

Il pacchetto di installazione di HCL BigFix contiene la versione Windows di BigFix Server, Client e Console. È necessario installare tali componenti nel computer con Windows 2016 e installare il client Windows nei computer con Windows 10.

Il pacchetto HCL BigFix Red Hat Client contiene la versione RHEL del BigFix Client ed è necessario per installare il BigFix Client sui computer con RHEL 7.

Il file LicenseAuthorization.BESLicenseAuthorization consente di creare la licenza BigFix effettiva per l'installazione specifica del server. Il file viene elaborato dal programma di installazione di BigFix.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

I risultati dei test del Fornitore sono stati generati per BigFix 10.0.1.41 su una piattaforma hardware conforme a quanto dichiarato nel Traguardo di Sicurezza [TDS]. Il Fornitore ha eseguito i suoi test utilizzando la versione e la configurazione dell'ODV, come definito nella guida CC [BFCCCG].

Il piano dei test del Fornitore elenca i casi di test per gruppi di SFR. La mappatura fornita elenca gli SFR e i casi di test per le TSFI corrispondenti. Il piano dei test è incentrato sulle funzioni di sicurezza dell'ODV. I casi di test sono mappati alle specifiche funzionali e ai sottosistemi corrispondenti. Alcuni test sono automatizzati. Ogni caso di test può contenere diversi test di una stessa funzione, concentrandosi su parti diverse (ad esempio, funzionalità di base, comportamento con parametri illegali e reazione a privilegi mancanti). Ogni test all'interno dei report di un caso di test è considerato PASS se le

condizioni indicate nella documentazione del caso di test sono soddisfatte, altrimenti viene segnalato come FAIL.

11.2.2 Copertura dei test

Nelle specifiche funzionali dell'ODV sono identificate le seguenti TSFI:

- Besadmin CLI
- BigFix Client
- Console
- REST API
- Client Register
- BigFix Site Administrator
- BigFix Relay
- OpenSSL (Server, Relay, Client)

La mappatura dei test del Fornitore mostra che questi coprono tutte le singole TSFI identificate.

11.2.3 Risultati dei test

Come descritto nell'approccio adottato per i test, i risultati dei test vengono scritti in documenti o memorizzati sotto forma di screenshot. Tutti i risultati dei test effettuati sull'ambiente di test mostrano che i risultati ottenuti sono identici ai risultati attesi; quindi tutti i test possono essere considerati superati.

I Valutatori hanno verificato che i test del Fornitore sono stati eseguiti su HW/SW conforme al Traguardo di Sicurezza [TDS]. I Valutatori sono stati in grado di seguire e comprendere appieno l'approccio adottato per i test del Fornitore utilizzando la documentazione dei test fornita. I Valutatori hanno analizzato la copertura e la profondità dei test del Fornitore esaminando tutti i casi di test. I Valutatori hanno verificato che l'estensione dei test del TSF copre le TSFI identificate nelle specifiche funzionali, incluse le interfacce interne dei sottosistemi. I Valutatori hanno esaminato i risultati dei test del Fornitore e li hanno trovati coerenti con i risultati attesi inclusi nel piano di test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

I Valutatori hanno configurato il sistema di test in base alla documentazione del Fornitore e al piano di test. La guida CC [BFCCCG] è stata preliminarmente valutata e ne è stata verificata la coerenza con il Traguardo di Sicurezza [TDS]. I Valutatori hanno configurato personalmente sia l'ODV, sia l'ambiente operativo, a garanzia che la configurazione per i test dei Valutatori fosse coerente con il TDS.

L'attività di test dei Valutatori è consistita di due fasi. In una prima fase è stato eseguito un sottoinsieme dei test del Fornitore, mentre in una seconda fase sono stati eseguiti i test

progettati dai Valutatori. Il sottoinsieme selezionato dei test del Fornitore ha incluso i test automatizzati del Fornitore. Tuttavia, i Valutatori hanno ripetuto i test automatizzati del Fornitore in modalità manuale, a causa dell'impossibilità per i Valutatori, a causa delle politiche interne del Fornitore, di accedere alla rete di HCL dove è installato il sistema di test automatico. Tutti i risultati dei test sono risultati conformi a quelli previsti dal piano di test del Fornitore.

Durante la revisione da parte dei Valutatori dei casi dei test del Fornitore, i Valutatori hanno verificato l'impegno del Fornitore nell'attività di test in ternini sia di profondità, sia di copertura in tutti i casi di test forniti. L'analisi ha mostrato una copertura molto ampia del TSF, per cui i Valutatori hanno progettato un numero ridotto di casi di test, rispetto alla quantità delle funzionalità dichiarate per la valutazione. I Valutatori hanno previsto in particolare i seguenti test:

- Alcuni controlli operativi aggiuntivi sui privilegi di utente di base per le API REST e la Console.
- Test aggiuntivi su BESAdmin.exe (hotfix).
- Test di autenticazione aggiuntivi sulle interfacce CLI.
- Un ulteriore test sull'autenticazione mediante API REST utilizzando stringhe non corrette.
- Test aggiuntivi sul parsing di input XML malformato da parte delle API REST e della CLI IEM.

Tutti i test predisposti dai Valutatori hanno avuto esito positivo.

11.4 Analisi di vulnerabilità e test di intrusione

La configurazione adottata per i test di intrusione è stata la stessa utilizzata per i test indipendenti, coerente con la configurazione valutata come specificato nel Traguardo di Sicurezza [TDS]. Anche l'ambiente operativo dell'ODV è stato verificato per i test di intrusione.

I Valutatori hanno esaminato inizialmente il Traguardo di Sicurezza e la documentazione di guida per identificare potenziali vettori di attacco. Sulla base di questa analisi, i Valutatori hanno stabilito che, per quanto riguarda la sicurezza fisica dell'ODV, attaccanti o utenti legittimi potrebbero potenzialmente tentare di lanciare attacchi tramite l'interfaccia dell'Administration Tool. L'interfaccia dell'ODV della BigFix Console si è rivelata non essere un possibile vettore di attacco.

I Valutatori hanno deciso di considerare i seguenti vettori logici di attacco per effettuare una ricerca pubblica di vulnerabilità con riferimento allo stack protocollare ISO/OSI:

- Livello di trasporto: UDP per BigFix Client (che è anche presente su BigFix Server), TLS1.2 per tutte le comunicazioni dei componenti dell'ODV.
- Livello applicazione: HTTP REST API, HTTPS REST API.

Allo scopo di individuare vulnerabilità potenziali, i Valutatori hanno utilizzato diverse parole chiave nel motore di ricerca di Google e in vari database di vulnerabilità, inclusi Common Vulnerabilities and Exposures (CVE), Exploit Database (EDB), Packet Storm (PS), SecurityFocus (SF) e HCL Customer Support. I Valutatori hanno rilevato 12 vulnerabilità potenziali su cui indagare ulteriormente.

La successiva analisi delle vulnerabilità potenziali ha portato a concludere che nessuna di queste è applicabile all'ODV. In particolare, è stato possibile escludere due vulnerabilità in quanto relative a librerie che non fanno parte dell'ODV, tre vulnerabilità risultate non sfruttabili nella configurazione valutata, quattro vulnerabilità risolte con la corretta applicazione di patch nella versione 10.0.1 di BigFix, una vulnerabilità non applicabile ipotizzando che gli amministratori dell'ODV siano formati, competenti e consapevoli delle politiche di sicurezza dell'organizzazione (ipotesi dell'ambiente operativo) e due vulnerabilità della versione TLS utilizzata nell'ODV non sfruttabili in quanto relative ad una funzione mai chiamata dall'ODV o gestite correttamente da un gestore degli errori nel codice di BigFix. Queste ultime due vulnerabilità sono state verificate esaminando il codice sorgente di BigFix.

I Valutatori hanno proseguito l'analisi delle vulnerabilità dell'ODV utilizzando la documentazione di guida, le specifiche funzionali, la progettazione dell'ODV e la descrizione dell'architettura di sicurezza per identificare potenziali vulnerabilità da indagare ulteriormente mediante i test di intrusione. Tuttavia, nessun documento ha rivelato possibili falle o difetti evidenti. I Valutatori si sono quindi concentrati su funzioni complesse dell'ODV che potrebbero includere possibili implementazioni errate e hanno selezionato le seguenti strategie per i test di intrusione:

- UDP fuzzing sull'interfaccia del Client
- REST API fuzzing / Path Traversal
- Sniffing tra component dell'ODV

Per il fuzzing / Path Traversal dell'e API REST sono stati utilizzati gli strumenti fuzzcat e sFuzz, mentre per intercettare il traffico tra i componenti dell'ODV è stato utilizzato Wireshark. I Valutatori hanno scelto di applicare tecniche di fuzzing a specifiche TSFI, per identificare difetti all'interno dell'ODV.

Al termine di tutte le sessioni di test di intrusione svolte, i Valutatori hanno potuto concludere che nessuno scenario di attacco con potenziale High o inferiore può essere portato a termine con successo nell'ambiente operativo dell'ODV nel suo complesso.

Al termine delle sessioni di test di intrusione, non è stata rilevata alcuna vulnerabilità sfruttabile nell'ambiente operativo previsto dell'ODV da parte di attaccanti con potenziale di attacco Basic. I Valutatori non hanno inoltre identificato alcuna vulnerabilità residua.