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. 2/20

(Certification No.)

Prodotto: Forcepoint Data Guard v3.0

(Product)

Sviluppato da: Forcepoint LLC

(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:

EAL4+
(ALC_FLR.2)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente da:Eva Spina
Organizzazione:MISE/80230390587
Data:26/05/2020 11:58:31

Roma, 26 maggio 2020

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

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

Forcepoint Data Guard v3.0

OCSI/CERT/CCL/05/2019/RC

Versione 1.0

26 maggio 2020

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	26/05/2020

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CD-ROM	Compact Disc - Read-Only Memory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DFM	Data Flow Manager
DFP	Data Filtering Process
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
GB	Gigabyte
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
INPA	Inbound Network Protocol Adaptor
IP	Internet Protocol
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
NPA	Network Protocol Adapter
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
ONPA	Outbound Network Protocol Adaptor
PP	Profilo di Protezione
RFV	Rapporto Finale di Valutazione
RHEL	Red Hat Enterprise Linux
RO	Read-Only

RW	Read-Write
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
TCP	Transmission Control Protocol
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
UDP	User Datagram Protocol

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2012-09-003, “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-2012-09-004, “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

[GADM] “Forcepoint Data Guard Administrator’s Guide”, Version 3.0.0.0-9005, 28 February 2019

[GCCS] “Forcepoint Data Guard Guidance Documentation Supplement”, Version 0.2, 6 November 2019

[RFV] “Forcepoint Data Guard v3.0” Evaluation Technical Report, v1, CCLab Software Laboratory, 14 April 2020

[TDS] “Forcepoint LLC Forcepoint Data Guard v3.0 Security Target”, Version 0.8, Corsec Security, Inc., 16 March 2020

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 fino a EAL4.

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 http://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 a EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Forcepoint Data Guard v3.0", sviluppato dalla società Forcepoint LLC, nel seguito del documento anche indicato come "Forcepoint Data Guard" o "FDG".

L'ODV è un prodotto software progettato per ispezionare, convalidare e filtrare il traffico di rete utilizzando un motore di regole flessibile che consente agli amministratori di implementare politiche per la protezione e la condivisione di dati aziendali.

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. 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 EAL4, 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 "Forcepoint Data Guard v3.0" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti 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	Forcepoint Data Guard v3.0.0.0 Build Number 9005
Traguardo di Sicurezza	"Forcepoint LLC Forcepoint Data Guard v3.0 Security Target", Version 0.8 [TDS]
Livello di garanzia	EAL4 con l'aggiunta di ALC_FLR.2
Fornitore	Forcepoint LLC
Committente	Corsec Security, Inc.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	7 ottobre 2019
Data di fine della valutazione	15 aprile 2020

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 "Forcepoint Data Guard v3.0" (FDG) è un prodotto esclusivamente software progettato per ispezionare, convalidare e filtrare il traffico di rete utilizzando un motore di

regole flessibile basato su Lua che consente agli amministratori di implementare politiche per la protezione e la condivisione di dati aziendali.

L'ODV gira su apparati hardware di tipo server disponibili in commercio e si colloca tra domini o reti con diversi livelli di sicurezza o classifica. L'ODV include solo l'applicazione software FDG. L'ODV ispeziona e filtra i flussi di dati in transito applicando le regole di filtraggio al traffico che fluisce tra gli adattatori di rete (NPA). Per impostazione predefinita, nessun dato può fluire tra gli NPA a meno che le regole non consentano il flusso.

Gli amministratori implementano regole per definire flussi unidirezionali o bidirezionali. Le regole di filtraggio per consentire o eliminare un *payload* di dati possono essere applicate a partire da un livello elevato (interfaccia, zona di rete o protocollo) fino al livello dei byte per un'ispezione approfondita del contenuto.

Per una descrizione dettagliata dell'ODV, si faccia riferimento ai par. 1.3, 1.4, 1.5 e 1.6 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riassunti di seguito.

7.3.1 Architettura dell'ODV

L'ODV è suddiviso nei seguenti componenti:

- Data Flow Manager (DFM)
- Data Filtering Process (DFP)
- Inbound Network Protocol Adaptor (INPA)
- Outbound Network Protocol Adaptor (ONPA)

Il componente DFM è l'elemento centrale per la creazione ed il monitoraggio dei processi della *pipeline* di filtraggio. I processi vengono creati in base alle definizioni dei flussi di dati. Il DFM avvia i processi INPA, DFP e ONPA e ne verifica lo stato di esecuzione. Il DFM fornisce inoltre un'interfaccia a linea di comando (CLI) per consentire agli amministratori di controllare il DFM stesso e di impostare i file di configurazione per tutti i componenti.

Gli amministratori utilizzano la CLI dell'ODV per configurare diverse impostazioni, tra cui quelle per consentire il traffico tra sorgenti e destinazioni, applicare politiche di flusso dei dati e importare le regole di filtraggio utilizzate per ispezionare e convalidare i flussi di dati. La CLI dell'ODV fornisce inoltre strumenti di gestione e monitoraggio dei flussi di dati che consentono di avviare e arrestare il processo di filtraggio e di ottenere dati relativi al trasporto dei flussi di dati e statistiche sui filtri.

Il componente DFP fornisce le funzionalità di filtraggio di base all'ODV. Il DFP gestisce le operazioni di input/output per i flussi di dati e implementa il motore di filtraggio basato su Lua. Gli amministratori implementano set di regole per convalidare i dati che fluiscono attraverso il motore di filtraggio, che può essere utilizzato per concatenare più filtri DFP.

Il DFP riceve i *payload* dei dati dall'INPA e applica le regole di filtro per determinare se i dati devono essere fatti passare o eliminati. Se i dati superano la convalida, vengono passati all'ONPA.

Il componente INPA riceve il traffico dall'*endpoint* di una sorgente esterna tramite una connessione UDP o TCP. L'INPA estrae il *payload* dei dati e verifica le politiche di flusso dei dati configurate prima di inviare i dati consentiti al DFP per il filtraggio.

Il componente ONPA riceve il *payload* dei dati dal DFP e verifica le politiche di flusso dei dati configurate prima di inviare il *payload* all'*endpoint* di una destinazione esterna utilizzando una connessione UDP o TCP.

La Figura 1 mostra l'ambito e i confini fisici dell'ODV.

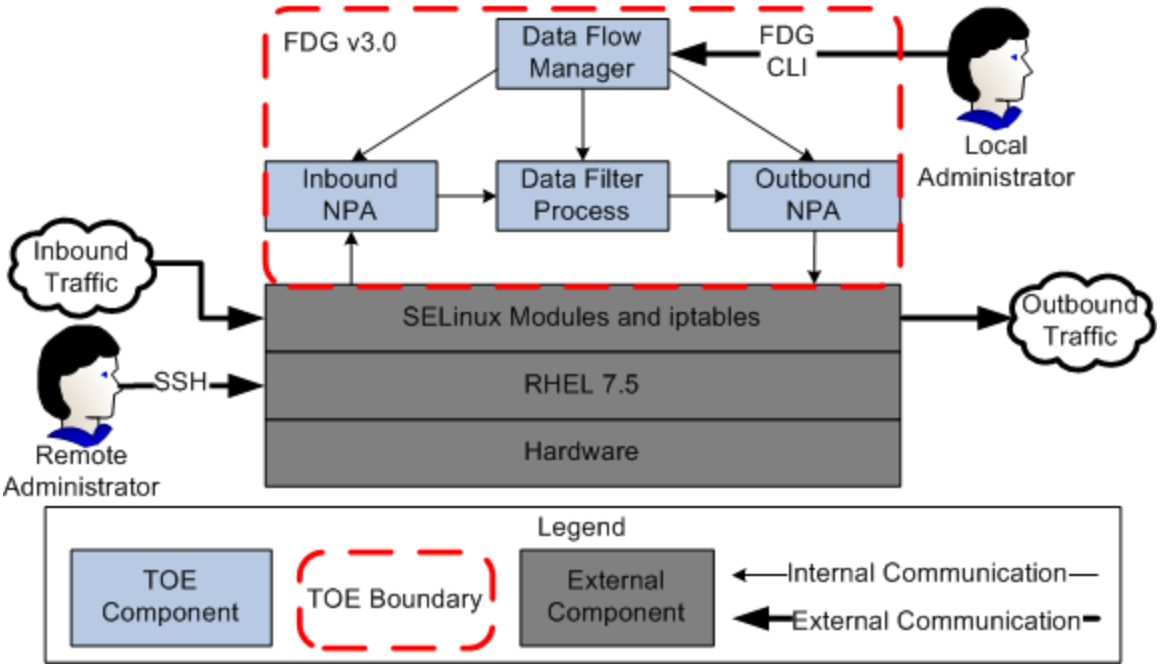

Figura 1 - Confini fisici dell'ODV

L'ODV gira sul sistema operativo RHEL 7.5. RHEL fornisce servizi di base quali autenticazione, archiviazione dati, SSH per l'autenticazione remota e il supporto di rete TCP/IP.

L'ODV viene gestito mediante la CLI a cui è possibile accedere attraverso una connessione SSH remota o utilizzando la console locale di RHEL.

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. 7.1 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Audit**: la funzionalità di audit dell'ODV registra gli eventi di avvio e arresto della funzione di audit, le modifiche alla configurazione e gli eventi relativi ai flussi di dati. Gli amministratori possono visualizzare i *log* di audit mediante la CLI dell'ODV.
- **Protezione dei dati degli utenti**: il controllo del flusso delle informazioni è implementato dall'ODV mediante le seguenti SFP: INPA Information Flow SFP

(INPA SFP), ONPA Information Flow SFP (ONPA SFP) e Flow SFP. La INPA SFP controlla il flusso di dati in entrata da una rete esterna. La ONPA SFP controlla il flusso di dati in uscita verso una rete esterna. La Flow SFP controlla ciò che può passare tra INPA e ONPA dopo che i dati sono stati filtrati dal DFP. Per impostazione predefinita, non è ammesso il passaggio di nessun dato a meno che il flusso non sia definito e consentito. Un amministratore con ruolo *read-write* (RW) definisce le regole di filtraggio dei flussi usando il linguaggio di *scripting* Lua e importa le regole nel formato di file Lua.

- **Identificazione e Autenticazione**: gli amministratori devono essere identificati dai loro ruoli nell'ODV prima di ottenere l'accesso a qualsiasi dato o funzionalità dell'ODV.
- **Gestione della sicurezza**: l'ODV permette di gestire le funzionalità di sicurezza, i dati del TSF e gli attributi di sicurezza dell'ODV. L'ODV fornisce i ruoli *read-only* (RO) e *read-write* (RW). Il ruolo *read-only* accede a funzionalità limitate per visualizzare i dati del TSF. Il ruolo *read-write* accede a funzionalità amministrative complete per la gestione del TSF. Un amministratore con ruolo *read-only* viene definito amministratore RO. Un amministratore con ruolo *read-write* viene definito amministratore RW. Il termine generico "amministratore", quando non è qualificato da RO o RW, si riferisce ad entrambi i ruoli.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto viene fornita all'utente finale insieme al prodotto. Questa documentazione contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti 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 Funzionali (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

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

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, 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 CCLab Software Laboratory.

L'attività di valutazione è terminata in data 15 aprile 2020 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 27 aprile 2020. 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 "Forcepoint Data Guard v3.0" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, 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 EAL4, 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
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	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
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo
Delivery procedures	ALC_DEL.1	Positivo

Classi e componenti di garanzia		Verdetto
Identification of security measures	ALC_DVS.1	Positivo
Flaw reporting procedures	*ALC_FLR.2*	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Focused vulnerability analysis	AVA_VAN.3	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 "Forcepoint Data Guard v3.0" 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 tutte le ipotesi descritte 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, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'installazione e all'utilizzo sicuro del prodotto in accordo con la documentazione di guida fornita insieme all'ODV ([GADM], [GCCS]).

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

L'ODV viene distribuito agli utenti finali in due modalità: su CD-ROM (distribuzione fisica) o come download (distribuzione digitale).

L'imballaggio e la spedizione dei supporti fisici avvengono tramite servizi di spedizione internazionali. Il Product Distribution Team di Forcepoint effettua la tracciatura dei pacchi a garanzia dell'accettazione della consegna. Il CD di installazione e il CD della documentazione sono inseriti in custodie per supporti in vinile, insieme a una copia del contratto di licenza del software (Forcepoint Software License Agreement), della lettera di accompagnamento del prodotto e del contratto di manutenzione del software (Forcepoint Software Maintenance Agreement). Questi articoli sono contenuti nel pacchetto dei supporti di installazione (Installation Media Packet), che è sigillato con un'etichetta a prova di manomissione. Questo pacchetto viene inserito in una busta di Manila imbottita, a sua volta inserita in un pacco del corriere per la spedizione.

Alla ricezione del pacchetto, un amministratore verifica l'integrità del CD di installazione (*fdg_3-0-0-0-9005_GA_2019-02-28*) e del CD della documentazione (*fdg_3-0-0-0-9005_Documentation_2019-02-28*) calcolando e verificando i loro *checksum* SHA-256.

Per gli ordini che richiedono la distribuzione digitale, l'ODV è fornito in formato immagine disco ISO. Tutti i download digitali vengono effettuati tramite link alla piattaforma Kiteworks. Le cartelle con i file necessari vengono create su Kiteworks e ne viene limitato l'accesso al Product Distribution Team e al cliente che le dovrà scaricare. I link di Kiteworks sono temporanei e durano al massimo una settimana prima che ne scada la validità. Il cliente scarica il software dal link dedicato connettendosi a Kiteworks in HTTPS.

Dopo aver scaricato i file immagine in formato ISO, l'amministratore verifica l'integrità del file di installazione (*fdg_3-0-0-0-9005_GA_2019-02-28.iso*) e del file della documentazione (*fdg_3-0-0-0-9005_Documentation_2019-02-28.iso*) calcolando e verificando i loro *checksum* SHA-256.

La verifica dei valori di *checksum* richiede che il cliente contatti Forcepoint.

9.2 Identificazione dell'ODV

Dopo l'installazione, la versione effettiva dell'ODV può essere verificata dalla CLI di FDG mediante il comando "show version". Il comando deve restituire la seguente stringa:

```
Forcepoint Data Guard 3.0.0.0-9005
```

9.3 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

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

In particolare, i seguenti documenti contengono informazioni dettagliate per la preparazione dell'ambiente operativo dell'ODV e l'inizializzazione sicura dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- "Forcepoint Data Guard Administrator's Guide", Version 3.0.0.0-9005, 28 February 2019 [GADM]
- "Forcepoint Data Guard Guidance Documentation Supplement", Version 0.2, 6 November 2019 [GCCS]

10 Appendice B – Configurazione valutata

L'ODV è il prodotto software "Forcepoint Data Guard v3.0", sviluppato da Forcepoint LLC.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] come "Forcepoint Data Guard v3.0.0.0 Build Number 9005". Il nome, il numero di versione e il numero di *build* identificano univocamente l'ODV.

L'ODV ha una sola configurazione valutata, verificata dai Valutatori all'atto dell'effettuazione dei test e a cui si applicano i risultati della valutazione stessa.

Per maggiori dettagli, consultare anche il par. 1.4 del Traguardo di Sicurezza [TDS].

10.1 Ambiente operativo dell'ODV

In Tabella 2 sono riportati sinteticamente i requisiti minimi dell'ambiente operativo dell'ODV per consentirne la corretta operatività. La presenza di reti in entrata e in uscita è necessaria all'ODV per la funzionalità di filtraggio del traffico.

Per maggiori dettagli, consultare anche il par. 1.5 del Traguardo di Sicurezza [TDS].

Componente	**Requisiti**
Sistema Operativo	Red Hat Enterprise Linux (RHEL) 7.5 con inclusi i seguenti elementi: • SELinux • Iptables • OpenSSH Server
Hardware	I requisiti minimi hardware includono i seguenti elementi: • Almeno una scheda di interfaccia di rete • Un lettore CD • 2 GB di memoria • 40 GB di spazio di archiviazione Per i requisiti hardware minimi di RHEL 7.5 si faccia riferimento a https://access.redhat.com/articles/rhel-limits.

Tabella 2 - Componenti dell'ambiente operativo dell'ODV

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 EAL4, con l'aggiunta di ALC_FLR.2, tali attività prevedono tre passi successivi:

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

11.1 Configurazione per i Test

Tutte le attività di test sono state svolte presso la sede dell'LVS.

Per l'esecuzione dei test il Fornitore ha messo a disposizione dell'LVS un insieme di risorse equivalente a quelle utilizzate per effettuare i suoi test.

I Valutatori hanno creato l'ambiente di test in conformità alla descrizione contenuta nella documentazione di test del Fornitore. Oltre alle apparecchiature descritte nel Traguardo di Sicurezza [TDS] per l'ambiente operativo dell'ODV, l'ambiente di test ha richiesto l'installazione di due *host* Linux aggiuntivi utilizzati per veicolare il traffico attraverso l'ODV.

I Valutatori hanno installato e configurato l'ODV nell'ambiente di test seguendo le procedure preparatorie descritte nella documentazione operativa fornita, come indicato nel par. 9.3. Pertanto, l'ODV utilizzato per i test è risultato installato in modo corretto ed in uno stato noto.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

L'approccio adottato per i test dal Fornitore consiste nell'eseguire test funzionali per dimostrare che il TSF e le TSFI si comportano come specificato nel Traguardo di Sicurezza [TDS], nelle specifiche funzionali, nel progetto e nella descrizione dell'architettura di sicurezza dell'ODV.

Il Fornitore ha preferito creare casi di test che verificano più funzionalità dell'ODV alla volta, invece di creare meno casi di test separati per ogni funzionalità. Da ciò deriva che il numero di casi di test del Fornitore è ridotto, ma i test risultano comunque completi.

11.2.2 Copertura dei test

I Valutatori hanno esaminato il piano di test presentato dal Fornitore e hanno verificato la completa copertura dei requisiti funzionali (SFR) e delle TSFI descritte nelle specifiche funzionali.

11.2.3 Risultati dei test

I Valutatori hanno eseguito tutti i casi di test descritti nel piano di test presentato dal Fornitore, verificando positivamente il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

I Valutatori non hanno utilizzato strumenti di test particolari per sollecitare tutte le TSFI selezionate per i test indipendenti.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o inseriti in test più complessi che interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione.

Tutti i test indipendenti eseguiti dai Valutatori hanno dato esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali (par. 11.1).

I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quella indicata nel Traguardo di Sicurezza [TDS], par. 1.2.

In una prima fase, i Valutatori hanno effettuato delle ricerche utilizzando varie fonti di pubblico dominio, al fine di individuare eventuali vulnerabilità note applicabili all'ODV. È stata in questo modo identificata una potenziale vulnerabilità nel componente per il filtraggio dei dati DFP, una versione personalizzata dell'ambiente di *runtime* Lua integrata nel software dell'ODV.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa) al fine di evidenziare eventuali ulteriori vulnerabilità potenziali dell'ODV.

Da queste analisi, i Valutatori hanno effettivamente determinato la presenza di tre vulnerabilità potenziali:

1. risulta non applicata una *patch* per la vulnerabilità CVE-2014-5461;

2. i comandi CLI di FDG per il backup e l'esportazione dei file potrebbero fornire informazioni sullo stato interno e sulla configurazione dell'ODV;

3. i comandi CLI di FDG per il ripristino e l'importazione dei file potrebbero consentire una modifica esterna dei dati di configurazione dell'ODV, con conseguente accesso non autorizzato ed elevazione dei privilegi.

Sebbene le funzionalità di backup e ripristino di FDG non facciano parte dell'ODV, le vulnerabilità 2 e 3 potrebbero essere potenzialmente sfruttate per effettuare ulteriori attacchi al TSF.

I Valutatori hanno analizzato nel dettaglio le vulnerabilità potenziali identificate nei passaggi precedenti e hanno progettato diversi scenari di attacco e test di intrusione per verificare la loro effettiva sfruttabilità nell'ambiente operativo dell'ODV, considerando un potenziale di attacco Enhanced-Basic.

Al termine di tutte le sessioni di test di intrusione, i Valutatori hanno concluso che nessuno degli scenari di attacco ipotizzati con potenziale Enhanced-Basic o inferiore può essere portato a termine con successo nell'ambiente operativo dell'ODV nel suo complesso e tutte le vulnerabilità identificate sono considerate residue, vale a dire che potrebbero essere sfruttate solo da attaccanti con potenziale di attacco superiore a Enhanced-Basic.

In particolare, la vulnerabilità 1 richiede un potenziale di attacco Moderate e risulta non completamente sfruttabile, mentre le altre due richiedono un potenziale di attacco High per essere sfruttate con successo.