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. 5/21

(Certification No.)

Prodotto: Zeta Server v1.1.1

(Product)

Sviluppato da: Prolan Power Zrt.

(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:

Conforme a: Protection Profile for Application Software v1.3

(Conformant to)

(ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente
da Eva Spina
Data: 2021.09.07
13:28:21 +02'00'

Roma, 7 settembre 2021

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

Zeta Server v1.1.1

OCSI/CERT/CCL/01/2021/RC

Versione 1.0

7 settembre 2021

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	07/09/2021

2 Indice

3 Elenco degli acronimi

API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIAP	National Information Assurance Partnership
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OS	Operating System
PII	Personally Identifiable Information
PP	Protection Profile
RAM	Random Access Memory
RFV	Rapporto Finale di Valutazione
RPM	Red Hat Package Manager
SAR	Security Assurance Requirement
SCADA	Supervisory Control And Data Acquisition
SFP	Security Function Policy

SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
SSL	Secure Sockets Layer
ST	Security Target
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Functionality
ZSC	Zeta Substation Controller
ZCM	Zeta Client Manager

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

[AGD] "Guidance Documentation - Zeta Server v1.1.1", v0.4, Prolan Power, 18 June 2021

[PP-APP] Protection Profile for Application Software, Version 1.3, NIAP, 1st March 2019

[RFV] "Zeta Server 1.1.1" Evaluation Technical Report, v1, CCLab Software Laboratory, 30 June 2021

[TDS] "Security Target - Zeta Server v1.1.1", v1.3, Prolan Power, 18 June 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 per tutti i componenti di garanzia dichiarati inclusi nel livello EAL1.

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 inclusi nel livello EAL1.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto software "Zeta Server v1.1.1", nel seguito del documento anche indicato come "Zeta Server", sviluppato dalla società Prolan Power Zrt.

L'ODV è una soluzione di controllo di livello aziendale per il monitoraggio e la supervisione che raccoglie misurazioni analogiche e binarie di apparecchiature elettriche da un gateway di sottostazione e offre la possibilità di impartire comandi a tali apparecchiature, se necessario, tramite una Web GUI che facilita la visualizzazione della sottostazione

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 i componenti di garanzia inclusi nel PP [PP-APP], 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 "Zeta Server v1.1.1" 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	Zeta Server v1.1.1
Traguardo di Sicurezza	"Security Target - Zeta Server v1.1.1", v1.3 [TDS]
Livello di garanzia	Conforme a PP con i seguenti componenti di garanzia: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1 e AVA_VAN.1
Fornitore	Prolan Power Zrt.
Committente	Prolan Power Zrt.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	Protection Profile for Application Software, Version 1.3 [PP-APP]
Data di inizio della valutazione	19 marzo 2021
Data di fine della valutazione	30 giugno 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 "Zeta Server v1.1.1" è una soluzione di controllo di livello aziendale (SCADA) per il monitoraggio e la supervisione che raccoglie misurazioni analogiche e binarie di apparecchiature elettriche da un gateway di sottostazione e offre la possibilità di impartire comandi a tali apparecchiature, se necessario, tramite una Web GUI che facilita la visualizzazione della sottostazione.

L'intera Zeta Solution è costituita dall'applicazione Zeta Server (l'ODV) e dal Substation Automation Gateway (SAGateway).

L'SAGateway si interfaccia con Zeta Server e ritrasmette i dati raccolti dalla sottostazione tramite vari protocolli di comunicazione standard, fornendo anche la possibilità di impartire comandi ai dispositivi IT. In assenza di questa connessione, la funzionalità di Zeta Server risulta molto limitata. L'SAGateway non fa parte dell'ODV.

7.3.1 Architettura dell'ODV

Zeta Server (l'ODV) è costituito dai seguenti sottosistemi:

- **Zeta Substation Controller (ZSC)**: si basa essenzialmente sui dati raccolti dal Substation Automation Gateway ed è responsabile di calcoli applicativi aggiuntivi che forniscono le informazioni necessarie per la visualizzazione della Web GUI ritrasmessa tramite lo Zeta Client Manager.

- **Zeta Client Manager (ZCM)**: è un'applicazione Web server che fornisce, in base al ruolo dell'utente, i dati necessari ai client per la visualizzazione della sottostazione tramite connessione SSL sicura. Inoltre, si interfaccia con lo Zeta Substation Controller per ritrasmettere i messaggi relativi alla sottostazione ai client e autorizza altresì i messaggi provenienti dai client inoltrandoli allo Zeta Substation Controller. Questo componente software è responsabile della maggior parte delle funzioni di sicurezza lato server.

La **Web GUI** è il modulo più importante di ZCM. Gli utenti autorizzati possono accedere tramite il loro browser Web ad una rappresentazione visuale dello stato attuale della sottostazione e sfruttare le funzionalità fornite dal software per ottenere informazioni dettagliate sui dispositivi IT, essere informati su modifiche importanti e immediatamente allarmati in caso di comportamenti imprevisti. Questa interfaccia di solito consiste in molte viste a seconda del modello di sottostazione, con vari contenuti che aiutano gli operatori a concentrarsi su diversi sottoinsiemi di dispositivi IT o sull'intera sottostazione. Molte delle impostazioni relative alla sicurezza possono essere modificate tramite la pagina di amministrazione della sicurezza. Gli utenti possono anche gestire i Substation Model nelle pagine di gestione corrispondenti.

Il **Substation Model** descrive le impostazioni di Zeta Server e il contenuto visualizzato della Web GUI. Include numerosi tipi di contenitori ed elementi ognuno dei quali rappresenta oggetti di funzioni realizzate, come topologie di sottostazione, viste, tipi di punti dati, tipi di eventi, elenchi di dati, relazioni di controllo-feedback, livelli di tensione, autorità del gruppo di utenti, ecc.

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 cap. 6 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Supporto crittografico**: l'ODV protegge i propri dati utilizzando il generatore di numeri casuali integrato nella piattaforma per generare identificatori di sessione, chiavi di cifratura delle password e altri valori casuali per difendersi da potenziali attacchi.

- **Protezione dei dati dell'utente**: l'ODV protegge i dati sensibili archiviati nella memoria non volatile. L'ODV limita il proprio accesso alla connettività di rete fornita dalle risorse hardware della piattaforma e non accede a nessuno degli archivi della piattaforma contenenti informazioni sensibili.

- **Gestione della sicurezza**: l'ODV viene fornito con credenziali predefinite e include una Web GUI per l'amministrazione degli utenti. L'utente Security Administrator può accedere alla Web GUI utilizzando credenziali predefinite e deve modificare immediatamente la propria password. Il Security Administrator può aggiungere o modificare utenti e impostare ruoli utente mediante la Web GUI.
  Gli account d'utente e le relative password sono archiviati in un database PostgreSQL sotto forma di *hash*.

- **Privacy**: l'ODV non gestisce informazioni che consentono l'identificazione personale (PII).

- **Protezione del TSF**: l'ODV è compatibile con il sistema operativo host della propria piattaforma quando questo è configurato in modo sicuro, utilizzando SELinux.
  L'ODV utilizza un set ben definito di API della piattaforma e librerie di terze parti. L'ODV consente al programma di installazione di verificare la propria versione e l'eventuale disponibilità di un aggiornamento. Per quest'ultimo controllo è necessaria una connessione a Internet.
  Gli aggiornamenti vengono distribuiti in formati appropriati per la piattaforma su cui è installato l'ODV. Questi sono firmati digitalmente e la firma viene convalidata prima dell'installazione. L'installazione di un aggiornamento dell'applicazione rimuove tutti i file installati in precedenza ad eccezione dei file di configurazione e di audit/log.

- **Canali e percorsi attendibili**: l'ODV utilizza il protocollo HTTPS per cifrare i dati in transito tra l'ODV stesso, i client e il Substation Automation Gateway. L'ODV si basa sull'implementazione della cifratura HTTPS fornita dalla piattaforma.

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. 8.3 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità *exact* al seguente Profilo di Protezione:

- Protection Profile for Application Software, Version 1.3 [PP-APP]

7.6 Requisiti funzionali e di garanzia

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

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

Considerando che il TDS dichiara conformità *exact* al PP [PP-APP], questo include anche il seguente componente di garanzia esteso definito in tale PP:

- ALC_TSU_EXT.1 (Timely Security Updates)

Il TDS include anche i seguenti componenti funzionali estesi definiti in [PP-APP]:

- FCS_RBG_EXT.1 (Random Bit Generation Services)
- FCS_CKM_EXT.1 (Cryptographic Key Generation Services)
- FCS_STO_EXT.1 (Storage of Credentials)
- FDP_DEC_EXT.1 (Access to Platform Resources)
- FDP_NET_EXT.1 (Network Communications)
- FDP_DAR_EXT.1 (Encryption of Sensitive Application Data)
- FMT_MEC_EXT.1 (Supported Configuration Mechanism)
- FMT_CFG_EXT.1 (Secure by Default Configuration)
- FPR_ANO_EXT.1 (User Consent for Transmission of Personally Identifiable Information)
- FPT_API_EXT.1 (Use of Supported Services and APIs)
- FPT_AEX_EXT.1 (Anti-Exploitation Capabilities)

- FPT_TUD_EXT.1 and FPT_TUD_EXT.2 (Integrity for Installation and Update)
- FPT_LIB_EXT.1 (Use of Third Party Libraries)
- FPT_IDV_EXT.1 (Software Identification and Versions)
- FTP_DIT_EXT.1 (Protection of Data in Transit)

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]. Inoltre, sono state eseguite tutte le attività di garanzia specifiche richieste dal PP [PP-APP].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS CCLab Software Laboratory.

L'attività di valutazione è terminata in data 30 giugno 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 26 luglio 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 CCLab Software Laboratory 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 "Zeta Server v1.1.1" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia definito dai SAR inclusi nel PP [PP-APP], 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 definito dai SAR inclusi nel PP [PP-APP].

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 for the operational environment	ASE_OBJ.1	Positivo
Stated security requirements	ASE_REQ.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Basic functional specification	ADV_FSP.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
Labelling of the TOE	ALC_CMC.1	Positivo
TOE CM coverage	ALC_CMS.1	Positivo
Timely Security Updates	*ALC_TSU_EXT.1*	Positivo
Test	**Classe ATE**	Positivo
Independent testing - conformance	ATE_IND.1	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability survey	AVA_VAN.1	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

8.2 Attività di garanzia aggiuntive

Il PP [PP-APP] include attività di garanzia aggiuntive che sono specifiche per la tipologia di ODV e sono richieste per la conformità *exact* al PP.

I Valutatori hanno svolto le attività di garanzia richieste per tutti gli SFR definiti nel PP [PP-APP] e inclusi nel Traguardo di Sicurezza [TDS]. L'obiettivo di queste sotto-attività è quello di determinare se sono soddisfatti tutti i requisiti delle attività di garanzia incluse nel PP.

I Valutatori hanno assegnato un verdetto "Positivo" a tutte le attività di garanzia incluse nel PP.

8.3 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "Zeta Server v1.1.1" 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 [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 una serie di raccomandazioni relative alla consegna, all'inizializzazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([AGD]).

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

L'ODV è composto unicamente da software e viene distribuito tramite download diretto dal sito Web del Fornitore. L'utente riceve le informazioni di accesso richieste come parte del processo di acquisto.

Una volta inserite le credenziali, l'utente deve cercare la categoria "ZETA binary package", scegliere la versione corrispondente all'ODV e cliccare sul pulsante di download. Il programma di installazione dell'ODV viene fornito come archivio ZIP.

Prima di installare o aggiornare l'ODV, il programma di installazione deve poter verificare che il pacchetto RPM rappresenti un'istanza completa del prodotto, provenga dal Fornitore e sia integro. A questo scopo, tutti i pacchetti forniti sono firmati digitalmente dal Fornitore e l'utente deve controllare la firma digitale prima che inizi il processo di installazione o aggiornamento.

Istruzioni precise su come verificare la firma digitale del pacchetto sono riportate nel capitolo 7 (Acceptance of the TOE) della documentazione di guida [AGD].

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione dell'ODV, la sua configurazione e la predisposizione dell'ambiente operativo devono essere eseguite dagli utenti secondo le istruzioni riportate nel seguente documento:

- "Guidance Documentation - Zeta Server v1.1.1", v0.4, 18 June 2021 [AGD]

La documentazione di guida [AGD] descrive anche le interfacce e le funzioni dell'ODV e fornisce informazioni sul loro utilizzo sicuro 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 software "Zeta Server v1.1.1", sviluppato da Prolan Power Zrt.

La configurazione valutata è costituita dal software dell'ODV e dalla documentazione di guida.

Gli elementi fisici dell'ODV sono i seguenti:

- Il file "Zeta_Server_1.1.1.zip", che include il pacchetto di installazione di Zeta Server e una directory di installazione contenente file di script aggiuntivi e file di configurazione dell'ambiente che supportano il processo di installazione.

- Il documento "Guidance Documentation - Zeta Server v1.1.1" [AGD].

Per maggiori dettagli si rimanda al par. 1.3 del Traguardo di Sicurezza [TDS].

10.1 Ambiente operativo dell'ODV

L'ambiente operativo dell'ODV include i seguenti elementi:

- La piattaforma su cui è installato l'ODV. L'ODV è in grado di funzionare su un sistema operativo Linux generico su un hardware di livello consumer.

- Altri componenti del prodotto. Il Substation Automation Gateway non è obbligatorio ma dovrebbe essere presente. Senza di esso la funzionalità dell'ODV è molto limitata.

- Un database PostgreSQL contenente dati degli utenti e delle applicazioni, log e cronologia dei valori di misura dei dispositivi della sottostazione.

L'ODV è progettato per funzionare su una piattaforma Linux CentOS 7 ed è stato valutato e sottoposto a test su questa specifica distribuzione Linux.

La piattaforma che ospita l'ODV ha i seguenti requisiti di sistema:

- processore a 4 core da 2 GHz;

- 8GB RAM;

- 1 GB di spazio minimo su disco.

Anche se l'ODV può essere installato su 1 GB di spazio libero, il Fornitore consiglia almeno 30 GB di spazio su disco per l'archiviazione dei log e della cronologia dei dati.

Per maggiori dettagli si rimanda al cap. 8 (TOE Installation) della documentazione di guida [AGD].

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 definito dai SAR inclusi nel PP [PP-APP], tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti e test di intrusione da parte dei Valutatori.

11.1 Configurazione per i test

Per le attività di test il Fornitore ha messo a disposizione una macchina virtuale e una Zeta Solution completa, i cui componenti principali sono Zeta Substation Controller (ZSC), Zeta Client Manager (ZCM), Web GUI, Substation Automation Gateway (SAGateway) e un Substation Model. L'SAGateway e il Substation Model non fanno parte dell'ODV.

Come primo passo, i Valutatori hanno scaricato la macchina virtuale dal sito Web del Fornitore, effettuando l'accesso con le credenziali fornite in precedenza dal Fornitore stesso. Tutti i file relativi alla valutazione sono disponibili separatamente sul sito.

Al termine del download, la macchina virtuale, che funge da sistema operativo, è stata importata nella piattaforma di virtualizzazione utilizzata per i test (VMware). L'accesso alla macchina virtuale ha richiesto l'uso di credenziali di login, anche queste fornite dal Fornitore. Successivamente, è stata verificata la firma digitale, è stato creato il database, sono stati generati i certificati, è stato configurato il server Web e infine è stato installato l'SAGateway per ottenere un ambiente operativo idoneo per l'ODV.

Infine, è stato installato il pacchetto RPM dell'ODV. I Valutatori hanno seguito le fasi di preparazione descritte nel cap. 8 della documentazione di guida [AGD] per realizzare una configurazione sicura dell'ODV.

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Il Traguardo di Sicurezza [TDS] dichiara conformità *exact* al PP [PP-APP], che definisce una serie casi di test mappati sugli SFR. I Valutatori hanno eseguito tutti i casi di test richiesti dal PP, soddisfacendo così anche i requisiti per ATE_IND.1.

Prima di iniziare l'attività di test, i Valutatori hanno verificato che l'ambiente di test fosse stato predisposto in maniera appropriata e che l'ODV fosse configurato correttamente.

I Valutatori hanno eseguito tutti i test richiesti descritti nei PP [PP-APP] e nelle Technical Decision del NIAP applicabili elencate nel par. 2.1 del Traguardo di Sicurezza [TDS].

Tutti i test eseguiti dai Valutatori hanno fornito risultati coerenti con i risultati attesi.

11.3 Analisi delle vulnerabilità e test di intrusione

In una prima fase, i Valutatori hanno utilizzato le tecniche cosiddette "Google dork" per cercare informazioni disponibili pubblicamente e vulnerabilità note dell'ODV. Per verificare quali informazioni fossero accessibili a un potenziale attaccante, i Valutatori hanno effettuato ricerche con le parole chiave "prolan power" e "zeta". I risultati di queste ricerche

non hanno fornito alcuna informazione significativa sull'ODV o su eventuali vulnerabilità sfruttabili.

I Valutatori hanno altresì esaminato il sito Web della società, ma non hanno trovato informazioni disponibili sull'ODV. Solo il componente SAGateway (che fa parte dell'ambiente operativo) risulta documentato.

Successivamente, i Valutatori hanno condotto una ricerca estesa per trovare vulnerabilità note che interessano le librerie di terze parti utilizzate dall'ODV, elencate nel cap. 9 del Traguardo di Sicurezza [TDS]. I Valutatori hanno eseguito una ricerca su Google e hanno anche verificato la disponibilità di exploit per le librerie di terze parti nei database di exploit accessibili pubblicamente.

Come risultato, sono state raccolte informazioni su tutte le vulnerabilità e gli exploit pubblicamente disponibili per l'ODV e le librerie di terze parti. Le vulnerabilità identificate sono state esaminate una per una. Sulla base di questa analisi, è stato selezionato un solo candidato per i test di penetrazione: Denial of Service tramite ZIP bomb (o "bomba a decompressione").

I Valutatori hanno cercato di sfruttare questa potenziale vulnerabilità, ma l'ODV ha dimostrato di resistere a questo tipo di attacco. I risultati dei test sono stati documentati e sufficientemente dettagliati per la ripetibilità.

I Valutatori hanno quindi concluso 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.