RELAZIONE DI VERIFICA

RNG

“Thunderkick”

25 Marzo 2016

INTRODUZIONE

I risultati presenti nel seguente report sono una sintesi delle verifiche descritte in altri documenti interni archiviati presso QUINEL. Il Richiedente dichiara che

- i file o moduli,
- le strutture delle basi dati e le funzionalità,
- i parametri contenuti nelle basi dati e in file di configurazione

oggetto delle verifiche ai fini della certificazione hanno lo stesso comportamento, finalità e valorizzazioni di quelli pubblicati.

Come espressamente richiesto dal Richiedente, sono stati valutati da QUINEL esclusivamente i punti prettamente statistici relativi all'estrazione dei numeri grezzi (int32) e dei numeri scalati in alcuni intervalli standard di numeri interi.

Quinel M non ha effettuato nessuna verifica relativamente alla mappatura dei risultati ne' all'integrazione dell'RNG con i giochi ne' le interazioni e/o integrazioni con eventuali giochi e relativi regolamenti.

Il Destinatario, accettando ed utilizzando questa Relazione di Verifica, dichiara di essere a conoscenza e di accettare senza riserve tutti i termini e le condizioni indicate a seguito. Qualora il Richiedente e/o il Destinatario non fossero d'accordo riguardo ai termini e le condizioni riportate, QUINEL si riserva di annullare la certificazione fornita con la presente Relazione di Verifica, ne consegue quindi che il Destinatario dovrà restituire immediatamente a QUINEL tutte le copie della presente e non potrà farne uso e riferimento alcuno.

SEZIONE 1

(informazioni generali che caratterizzano e contraddistinguono l'attività di verifica)

1. Identificativo della verifica

THK002RNG_20160325_CERT

2. Ente di verifica emittente del certificato

QUINEL M. LTD
Marina Court, Flat 8,
Triq Giuseppe Cali',
XBX 1421 Ta'Xbiex – Malta
VAT number MT 2115-0515

Sito della verifica:
Via Prampolini, 28
43044 Lemignano di Collecchio (PR)

3. Riferimento alle Linee Guida utilizzate per la verifica

Linee Guida per la certificazione della piattaforma di gioco – Versione 1.2 del 24 dicembre 2014– Decreto direttoriale 2011/666/Giochi/GAD

4. Nome e identificativo dell'oggetto verificato

RNG Thunderkick

5. Tipologia dell'oggetto verificato

Generatore di numeri casuali. Il RNG è sviluppato con tecnologia JAVA.

Le verifiche sono state effettuate utilizzando una applicazione di test apposita che chiama ricorsivamente l'RNG oggetto della verifica. Il simulatore è stato reso fruibile mediante (.jar) presso i laboratori Quinel M.

Il generatore di numeri casuali ricorsivamente interrogato presso i laboratori di QUINEL ha prodotto le stringhe necessarie per i test.

6. Descrizione dell'oggetto verificato

Random Number Generator

Tipo: software-based RNG
Linguaggio di programmazione: JAVA
Version: 3.5.0
Path: /casino/engine/RNG.php

Description of RNG:
Random number generator uses /dev/urandom to generate secure random numbers. /dev/urandom is a file that serves as a random number generator or as a pseudorandom number generator. /dev/urandom ("unlocked"/non-blocking random source) allows access to environmental noise collected from device drivers and other sources. The generator keeps an estimate of the number of bits of noise in the entropy pool. From this entropy pool random numbers are created. When read, the /dev/urandom device will only return random bytes within the estimated number of bits of noise in the entropy pool. When the entropy pool is empty /dev/urandom reuses the internal pool to produce more pseudo-random bits and does not block as his counterpart /dev/random.

Description of RNG source code:
The RNG source code consists of one class containing four methods. Class defined as RNG contains the following four methods:
- __construct()
- __destruct()

- get_rand()
- random()

Methods explained:

__construct()

Method is called when the object is created. Method binds a resource /dev/urandom, to stream in a variable $this->handle.

__destruct()

Method is called when there are no more visible usages of the object. Method closes the file pointed in a variable $this-handle.

get_rand($max = 22)

Method is static and can be called directly without creating a new object. Method takes one incoming parameter $max with a default value 22 which defines a highest possible return value. At the start method checks if the $max value is defined, if not stops and returns value -1, if defined continues with opening the /dev/urandom file and storing a resource in a variable $handle. Through a loop we gather random characters from /dev/urandom file and transform them into 8bit ASCII value, then joining them into a 32bit random number using left bit shift. If the number overflows and it is negative we convert it back to double positive. To get the number within a range of 0 to maximum passed value we have to divide randomly generated 32bit number with a maximum 32bit number and multiplying it with maximum value passed through an argument and discard the decimals. The method return a random value within a range of 0 to maximum passed to the method. The maximum passed number to the method must not exceed maximum 32bit number (4294967295).

random($max = 1)

Method random() takes one incoming parameter $max with a default value 1 which defines a highest possible return value. Method random() works similar to get_rand(). The difference between the two is that get_rand() is static and it can be called directly but each time get_time() is called it creates a new

/dev/urandom file resource and when finished closes the file pointer. Method random() requires object RNG to be created and when created the method __constructor() creates a file pointer handle and when the object isn't used anymore the __destructor() closes the file pointer. The random() method uses same handle (file pointer) to create multiple random numbers and is faster in the process then get_rand(), but it cannot be called directly.

RNG Seeding
The Linux kernel uses keyboard, mouse, network, and disc activities, with a cryptographic algorithm (SHA1), to Generate seed data for the /dev/random device. /dev/urandom uses small amounts of data from /dev/random to seed a secondary entropy pool. This has the effect of inflating the real entropy so it can be conserved. Using /dev/urandom can cause /dev/random's pool to become empty, but if this happens /dev/urandom will not block, and it will continue using the last available seed.

RNG Range
RNG produces random 32bit number. Range of RNG is between 0 and maximum 32bit number (4294967295).

RNG Period
The /dev/urandom device attempts to ensure that each number in the sequence of random numbers have no relationship with the next. This makes /dev/urandom highly unpredictable and RNG period cannot be calculated.

7. Estremi del produttore dell'oggetto verificato

THUNDERKICK MALTA LTD
Level 5, The Mall Complex
Floriana (Malta)

8. Estremi del richiedente della verifica

THUNDERKICK MALTA LTD
Level 5, The Mall Complex
Floriana (Malta)

9. Data di ricezione della richiesta di verifica

Data richiesta Verifica 22/03/2016

10. Data di completamento della verifica

Termine Verifica 25/03/2016

11. Esito

CONFORME

12. Altre annotazioni

L'engine di entropia utilizzato come singleton fornisce le sequenze numeriche ai vari giochi introducendo un ciclo di background a ulteriore garanzia dell'imprevedibilità dei risultati.

SEZIONE 2

(dettaglio dei componenti HW verificati)

1. Produttore

NON APPLICABILE

2. Identificativo del componente HW

NON APPLICABILE

3. Funzionalità che caratterizzano l'oggetto HW

NON APPLICABILE

4. Riferimento alla verifica effettuata

NON APPLICABILE

5. Altre annotazioni

NON APPLICABILE

SEZIONE 3

(dettaglio dei componenti SW verificati)

1. Produttore

THUNDERKICK MALTA LTD Level 5, The Mall Complex Floriana (Malta)

2. Identificativo del componente SW

Si faccia riferimento a Sezione 1 punto 4

3. Funzionalità che caratterizzano l'oggetto SW

I file compilati su cui dovrà essere effettuato il controllo quotidiano del digest

Nome file	Descrizione
rng-implementation\gp-rng-3.5.0-RELEASE.jar	Core del motore di entropia
rng-interface\gp-rng-api-3.5.0-RELEASE.jar	Interface di interfacciamento

4. Firma digitale

I FILE ELENCATI SONO STATI OGGETTO DI VERIFICA	
SHA1	**NOME FILE**
**********	rng-implementation\gp-rng-3.5.0-RELEASE.jar
**********	rng-interface\gp-rng-api-3.5.0-RELEASE.jar

I file elencati sono ritenuti critici e dovranno essere quindi sottoposti all'invio quotidiano dei message digest (830) come richiesto al punto 2.2.7 delle linee guida.

5. Eventuale % di RTP

NON APPLICABILE

6. Riferimento alla verifica effettuata

JOB N° THK002RNG Rif. Doc interno FORM-1.0.1- THK002RNG

7. Altre annotazioni

/

SEZIONE 4

(dettaglio delle verifiche eseguite)

1. Identificativo del prodotto

RNG per estrazione di numeri scalati.

2. Verifica eseguita

Le verifiche, che sono state eseguite, sono riportate in dettaglio nel documento interno QUINEL: FORM-1.0.1- THK002RNG.xls e sugli archivi Quinel.

A titolo indicativo ma non esaustivo sono stati effettuati i seguenti test:

Numeri scalati, sui seguenti range:
[0,36],
[0,51],
[0,99],
[0,149],
[0,199],
[0,249],

1) Test di distribuzione uniforme
2) Test di indipendenza statistica
3) Runs Test
4) Batteria di test automatici statistici tra cui Frequency test, Gap test, Order test, T-student test, Wilcox test e Shapiro test
5) Test di auto-correlazione interna
6) Test di cross-correlazione tra le differenti sequenze di numeri (stesso range)

Numeri grezzi (int32 bit):
7) Die Hard (Marsaglia test)
8) Nist
9) Analisi codice sorgente;

3. Esito

CONFORME

4. Altre annotazioni

/

SEZIONE 5

(elenco completo dei requisiti soddisfatti)

1. Requisiti generatore numeri casuali (RNG)

NOTE

(*): Il ciclo di background come dichiarato dal produttore sarà realizzato utilizzando un'unica istanza RNG alla quale faranno accesso i vari giochi.

Descrizione requisiti/funzionalità	Esito	Rif. linee guida
Prevedibilità rilevante o meno per l'applicazione specifica.	APPLICABILE	2.5
Caratteristiche generali del RNG.	CONFORME	2.5.1 Punto1
Caratteristiche generali del RNG.	NON VERIFICATO*	2.5.1 Punto2,3,4
Dimensionamento.	CONFORME	2.5.2
Mappatura.	CONFORME	2.5.3
RNG basato su software, hardware o una combinazione di entrambi.	CONFORME	2.5.4
Monitoraggio del RNG basato su hardware per evidenziarne gli eventuali guasti.	NON APPLICABILE	2.5.5
Requisiti di RNG basato sul software: – periodo sufficientemente ampio.	CONFORME	2.5.6 2.5.6.1
– intervallo di risultati grezzi sufficientemente ampio.	CONFORME	2.5.6.2
– metodi di generazione/rigenerazione tali da assicurare che i valori seme siano determinati in modalità sicura e non prevedibili.	CONFORME	2.5.6.3
Attività/ciclo in background (non applicabile ai giochi di abilità).	CONFORME(**)	2.5.7

SEZIONE 6

(informazioni complete relative alla dichiarazione di conformità)

CERTIFICAZIONE

THUNDERKICK MALTA LTD
Level 5, The Mall Complex
Floriana, Malta

Totale Numero di pagine: 15

Totale Numero di pagine: 15

QUINEL M ha verificato che il RNG e i files contenuti nella sezione 3.4, risultano essere conformi a quanto stabilito nelle Linee Guida per la certificazione della piattaforma di gioco - Versione 1.2 del 24 dicembre 2014 emanate da AAMS.

Requisiti: 2.5.1-1, 2.5.2, 2.5.3, 2.5.4, 2.5.6, 2.5.6.1, 2.5.6.2, 2.5.6.3, 2.5.7

Sono stati valutati da QUINEL esclusivamente gli aspetti delle sopracitate Linee Guida considerabili prettamente statistici per il RNG oggetto di certificazione e non la conformità delle interazioni e/o integrazioni con eventuali giochi e relativi regolamenti così come richiesto dal richiedente.

Data: 25 marzo 2016

Firma:

_____

Isacco Ceci
(QUINEL M LTD)

CONDIZIONI

1. Le verifiche sono state effettuate utilizzando una applicazione di test apposita che sfrutta il RNG oggetto della verifica sviluppata con tecnologia JAVA.

2. I range testati e utilizzati dall'algoritmo del RNG sono quelli specificati nella presente relazione.

3. Quinel M non ha effettuato verifiche relative alla infrastruttura hw/sw, i server e i sistemi operativi dell'ambiente di produzione. Tali verifiche saranno da effettuare al momento dell'integrazione dell'RNG con il gioco e/o con la piattaforma del concessionario.

4. Come richiesto dal Richiedente non sono stati condotti test relativamente ai punti 2.5.1-2,3,4 tali punti dovranno essere quindi valutati al momento della certificazione del gioco che utilizza l'oggetto della presente certificazione.

END
OF
DOCUMENT