Bundesamt
für Sicherheit in der
Informationstechnik

Übersicht über Linux-Kernel mit NTG.1-konformem Zufallszahlengenerator /dev/random

(Stand: Dezember 2017)

Im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat die atsec information security GmbH den Zufallszahlengenerator (engl. random number generator, kurz RNG) /dev/random von Linux auf seine kryptographische Eignung untersucht. Bei dieser Untersuchung handelt es sich um eine Dauеruntersuchung, d.h. der RNG von jedem neu erscheinenden Linux-Kern wird geprüft.

Im Rahmen dieser Analyse wird insbesondere untersucht, ob /dev/random die Anforderungen der Funktionalitätsklasse NTG.1 gemäß [AIS20_31] erfüllt. Dabei werden gewisse Annahmen an die Konfiguration des Linux-Kernels und die zugrunde liegende Plattform getroffen (siehe Hinweise). Der Untersuchungsbericht ist auf der BSI-Webseite verfügbar [LRNG].

Die folgende Tabelle enthält eine Übersicht der untersuchten Linux-Kernel sowie eine Aussage darüber, ob der zugehörige RNG /dev/random grundsätzlich für einen Nachweis der NTG.1-Konformität geeignet ist.

Kernel-Version	Konform zu NTG.1[1]	Berichts-Version	Kapitel im Bericht
Ubuntu Oneric Ocelot 3.2.0-26.41	Ja	0.3	
3.5	Ja	0.3	A.1
3.6	Ja	3.0	B.2
3.7	Ja	3.1	B.3
3.8	Ja	3.4	B.4
3.9	Ja	3.5	B.5
3.10	Ja	3.6	B.6
3.11	Ja	3.7	B.7
3.12	Ja	3.8	B.8
3.13	Ja	4.0	B.9
3.14	Ja	4.1	B.10
3.15	Nein	4.2	B.11
3.16	Nein	4.3	B.12
3.17	Ja	4.4	B.13
3.18	Ja	4.5	B.14
3.19	Ja	4.6	B.15

1 Nur bei Beachtung der Hinweise nach der Tabelle.

4.0	Ja	4.7	B.16
4.1	Ja	4.8	B.17
4.2	Ja	5.1	B.18
4.3	Ja	5.1	B.19
4.4	Ja	5.2	B.20
4.5	Ja	5.2	B.21
4.6	Ja	5.2	B.22
4.7	Ja	5.3	B.23
4.8	Ja	5.4	B.24

Die folgende Tabelle bezieht sich auf den neuen Bericht (in englischer Sprache). Es handelt sich hierbei um die Fortsetzung der Linux-RNG-Studie.

Kernel-Version	**Konform zu NTG.1**[2]	**Berichts-Version**	**Kapitel im Bericht**
4.9	Ja	1.0	
4.10	Ja	1.1	9.1
4.11	Ja	1.2	9.2
4.12	Ja	1.3	9.3
4.13	Ja	1.5	9.4
4.14	Ja	1.6	9.5

Wichtige Hinweise
Die Ergebnisse der Untersuchung [LRNG] sind nur dann auf den RNG /dev/random eines Linux-basierten Produkts anwendbar, wenn folgende Grundvoraussetzungen erfüllt sind:

1. Das Linux-System läuft auf einer x86-Plattform.
2. Die CPU des Systems verfügt über die RDTSC-Instruktion.
3. Die Taktfrequenz der CPU ist mindestens 1 GHz.
4. Das Linux-System läuft nicht in einer virtuellen Maschine.
5. Die für /dev/random relevanten Quelltext-Dateien des Kernels sind gegenüber der untersuchten Upstream-Version unverändert.

Darüber hinaus ist zu beachten, dass für eine Feststellung der NTG.1-Konformität die in der Studie getroffenen Annahmen erfüllt sein müssen. Beispielsweise muss der innere Zustand des RNG geschützt sein, es dürfen nur untersuchte Entropiequellen einen bewerteten Entropiebeitrag liefern etc.

Diese Eigenschaften können bei Bedarf im Rahmen eines Zertifizierungsverfahrens (z.B. Common Criteria) evaluiert werden.

2 Nur bei Beachtung der Hinweise nach der Tabelle.

Referenzen

[AIS20_31]	Wolfgang Killmann, Werner Schindler: *A proposal for: Functionality classes for random number generators*, Version 2.0, September 2011, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf
[LRNG]	*Dokumentation und Analyse des Linux-Pseudozufallszahlengenerators*, URL: https://www.bsi.bund.de/DE/Publikationen/Studien/LinuxRNG/index_htm.html