

Rapport préliminaire – Audit d'OpenSSL

Date	5 février 2014
Rédigé par	Claire Smets, William Boisseleau, Pascal Edouard, Mathieu Latimier, Julien Legras
À l'attention de	Ayoub Otmani

Table des matières

Introduction	5
1 Entropie	6
1.1 Définitions et contexte	6
1.2 Audits	6
1.2.1 Audit 1 : X	6
1.2.1.1 Norme visée	6
1.2.1.2 Faille	6
1.2.1.3 Implémentation	6
1.3 Recommandations générales	7
2 Génération des clés	8
2.1 Définitions et contexte	8
2.2 Audits	8
2.2.1 Audit 1 : X	8
2.2.1.1 Norme visée	8
2.2.1.2 Faille	8
2.2.1.3 Implémentation	8
2.3 Recommandations générales	9
3 Poignée de main	10
3.1 Définitions et contexte	10
3.2 Audits	10
3.2.1 Audit 1 : X	10
3.2.1.1 Norme visée	10
3.2.1.2 Faille	10
3.2.1.3 Implémentation	10
3.3 Recommandations générales	11
Conclusion	12

Table des figures

1.1	Titre de Figure 1.1	7
2.1	Titre de figure 2.1	9
3.1	Titre de figure 3.1	11

Listings

1.1	codeAleatoire.c	6
2.1	codeAleatoire.c	8
3.1	codeAleatoire.c	10

Introduction

Ceci est l'introduction

Chapitre 1

Entropie

1.1 Définitions et contexte

1.2 Audits

1.2.1 Audit 1 : X

1.2.1.1 Norme visée

1.2.1.2 Faille

1.2.1.3 Implémentation

Version OpenSSL.

Fonction.

La fonction liée à cette norme est accessible sous le paquetage `bla/bla/bla`, dont les composantes principales sont listées en *listing 3.1*.

```
1 #include <stdio.h>
2 #define N 10
3 /* Block
4  * comment */
5
6
7 int main()
8 {
9     int i;
10
11     // Line comment.
12     puts("Hello world!");
13
14     for (i = 0; i < N; i++)
15     {
16         puts("LaTeX is also great for programmers!");
17     }
18
19     return 0;
20 }
```

||

Listing 1.1 – codeAleatoire.c

Audit.

1.3 Recommandations générales



FIGURE 1.1 – Titre de Figure 1.1

Chapitre 2

Génération des clés

2.1 Définitions et contexte

2.2 Audits

2.2.1 Audit 1 : X

2.2.1.1 Norme visée

2.2.1.2 Faille

2.2.1.3 Implémentation

Version OpenSSL.

Fonction.

La fonction liée à cette norme est accessible sous le paquetage `bla/bla/bla`, dont les composantes principales sont listées en *listing 3.1*.

```
1 #include <stdio.h>
2 #define N 10
3 /* Block
4  * comment */
5
6
7 int main()
8 {
9     int i;
10
11     // Line comment.
12     puts("Hello world!");
13
14     for (i = 0; i < N; i++)
15     {
16         puts("LaTeX is also great for programmers!");
17     }
18
19     return 0;
20 }
```


||

Listing 2.1 – codeAleatoire.c

Audit.

2.3 Recommandations générales



FIGURE 2.1 – Titre de figure 2.1

Chapitre 3

Poignée de main

3.1 Définitions et contexte

3.2 Audits

3.2.1 Audit 1 : X

3.2.1.1 Norme visée

3.2.1.2 Faille

3.2.1.3 Implémentation

Version OpenSSL.

Fonction.

La fonction liée à cette norme est accessible sous le paquetage `bla/bla/bla`, dont les composantes principales sont listées en *listing 3.1*.

```
1  #include <stdio.h>
2  #define N 10
3  /* Block
4   * comment */
5
6  int main()
7  {
8      int i;
9
10     // Line comment.
11     puts("Hello world!");
12
13     for (i = 0; i < N; i++)
14     {
15         puts("LaTeX is also great for programmers!");
16     }
17
18     return 0;
19 }
```

||

Listing 3.1 – codeAleatoire.c

Audit.

3.3 Recommandations générales



FIGURE 3.1 – Titre de figure 3.1

Conclusion

Ceci est la conclusion