PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2010/07

KeePass
Version 2.10 Portable

Paris, le 19 janvier 2011

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CSPN-2010/07

Nom du produit

KeePass

Référence/version du produit

Version 2.10 Portable

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN, Phase expérimentale)

Développeur(s)

Dominique Reichl
Haydnstr.12
72555 Metzingen
Allemagne

Commanditaire

Agence nationale de la sécurité des systèmes d'information
Secrétariat Général de la Défense et de la Sécurité Nationale
51, boulevard de la Tour Maubourg
75700 – Paris – 07 SP
France

Centre d'évaluation

THALES
BPI 1414 18, avenue Edouard Belin 31401 Toulouse Cedex 9, France
Tél : +33 (0)5 62 88 28 01, mél : nathalie.feyt@thalesgroup.com

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1 Le produit

1.1 Présentation du produit

Le logiciel open source KeePass est un « coffre-fort » de mots de passe qu'il stocke dans une base de données dont l'accès est authentifié et le contenu chiffré.

1.1.1 Catégorie du produit

1 - détection d'intrusion
2 - anti-virus, protection contre les codes malicieux
3 – pare-feu
4 - effacement de données
5 - administration et supervision de la sécurité
6 - identification, authentification et contrôle d'accès
7 - communication sécurisée
8 - messagerie sécurisée
9 - stockage sécurisé
10 - matériel et logiciel embarqué

1.1.2 Identification du produit

Une fois installée, la version du produit est identifiable en cliquant sur la rubrique « A propos » du menu « Aide » de KeePass. Une boîte de dialogue apparaît en affichant la version du produit en caractère blanc.

1.1.3 Services de sécurité

Les fonctions de sécurité du logiciel Keepass sont les suivantes :

- génération de mots de passe robustes ;
- génération de clés maîtres robustes ;
- authentification de l'utilisateur (contrôle d'accès par mot de passe et/ou fichier clé) ;
- chiffrement/déchiffrement des données de la base de données ;
- intégrité de la base de données (protection et vérification) ;
- effacement des données temporaires ;

- chiffrement des données temporaires ;
- déconnexion automatique de la base de données pour prévenir une perte de données et un accès permanent à la base ;
- mécanisme d'« obfuscation » des mots de passe et des identifiants de connexion (par exemple « login » de compte Internet) à travers le presse-papiers et la simulation de frappe clavier.

1.1.4 Configuration évaluée

Sans objet.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation est menée conformément au référentiel « Certification de Sécurité de Premier Niveau en phase expérimentale ». Les références des documents se trouvent en annexe 2.

2.2 Charge de travail prévue et durée de l'évaluation

La charge de travail prévue lors de la demande de certification est conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours. L'évaluation s'est déroulée au cours du mois de septembre 2010.

2.3 Travaux d'évaluation

Ce paragraphe apporte des précisions sur le déroulement de l'évaluation et d'éventuels compléments sur la cible de sécurité [ST], issus du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1 Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1 Spécification de besoin du produit

Conforme à la cible de sécurité [ST].

2.3.1.2 Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [ST].

2.3.1.3 Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [ST].

2.3.1.4 Fonctions de sécurité

Conforme à la cible de sécurité [ST].

2.3.1.5 Hypothèses sur l'utilisation du produit

Conforme à la cible de sécurité [ST].

2.3.1.6 Utilisateurs typiques

Conforme à la cible de sécurité [ST].

2.3.2 Installation du produit

2.3.2.1 Plate-forme de test

Le produit a été évalué sous Windows XP SP3, Windows Vista et Windows Seven sur une machine virtuelle VirtualBox version 3.1.0 sous Windows XP SP3.

2.3.2.2 Particularités de paramétrage de l'environnement

Sans objet.

2.3.2.3 Options d'installation retenues pour le produit

Sans objet.

2.3.2.4 Description de l'installation et des non-conformités éventuelles

Sans objet.

2.3.2.5 Durée de l'installation

L'installation du produit est immédiate.

2.3.2.6 Notes et remarques diverses

Sans objet.

2.3.3 Analyse de la conformité

2.3.3.1 Analyse de la documentation

Les guides [GUIDES] sont clairs et exhaustifs.

2.3.3.2 Revue du code source

L'évaluateur estime que le code source est clair et bien structuré.

2.3.3.3 Fonctions testées

Le tableau ci-dessous reprend les tests menés lors de l'évaluation ainsi que les verdicts associés (***Réussite***, ***Échec*** ou ***Non Conclusif***).

Description de la fonction	**Résultat**
Génération de mot de passe	***Réussite***
Calcul de l'entropie du mot de passe	***Réussite***
Génération de clé maître	***Réussite***
Création d'une base de données et chiffrement/déchiffrement de la base à l'aide d'un mot de passe	***Réussite***
Création d'une base de données et chiffrement/déchiffrement de la base à l'aide d'un fichier clé	***Réussite***

Authentification de l'utilisateur (contrôle d'accès par mot de passe et/ou fichier clé)	***Réussite***
Effacement des données temporaires après verrouillage ou fermeture de la base	***Réussite***
Verrouillage ou fermeture automatique de la base de données après un temps donné.	***Réussite***
Journalisation des accès à la base	***Réussite***
Mécanisme d'« obfuscation » du presse-papier	***Réussite***

2.3.3.4 Synthèse des fonctions testées et non testées

Les fonctionnalités d'administration n'ont pas été testées car non applicables à la version « portable » du produit.
Les fonctionnalités d'export et d'import de fichiers de mots de passe (y compris les TAN[1]) et de téléchargement de plugins n'ont pas été testées.

2.3.3.5 Avis d'expert sur le produit

La documentation est complète. Le produit est conforme à sa cible de sécurité. Toutes les fonctionnalités testées sont conformes à la cible de sécurité.

2.3.4 Analyse de la résistance des mécanismes et des fonctions

2.3.4.1 Liste des fonctions testées et résistance

Génération du mot de passe utilisateur
L'attaque sur les mots de passe générés revient à une recherche exhaustive sur l'espace des mots de passe.

Protection de la base de données
KeePass utilise une clé dite « composée » pour assurer la confidentialité de la base de données. Cette clé est un condensat SHA 256 de divers clé que l'utilisateur peut sélectionner (fichier de clé, mot de passe, clé originaire de plugins).

2.3.4.2 Avis d'expert sur la résistance des mécanismes

Le mécanisme de protection de la base de données ne présente pas de vulnérabilité intrinsèque et repose entièrement sur l'entropie du mot de passe et du fichier de clé éventuel.

[1] Transaction Authentication Number, mots de passe qui ne peuvent être utilisés qu'une seule fois, principalement par les banques.

2.3.5 Analyse des vulnérabilités (conception, implémentation…)

2.3.5.1 Liste des vulnérabilités connues

KeePass est sensible à une vulnérabilité liée à certains composants de Windows tentant de charger des bibliothèques externes non existantes. Appelée « Insecure Library Loading » et référencée par Microsoft sous le code MSA 2269637, cette vulnérabilité est liée à un mécanisme standard qui, lors du chargement des bibliothèques, cherche automatiquement la librairie dwmapi.dll même lorsqu'elle n'est pas indispensable au fonctionnement du logiciel. Cette dernière gère des éléments d'affichage du bureau sous Windows Vista et n'existe pas dans les versions antérieures de l'OS. Dans le cas où elle n'est pas présente dans le répertoire système, Keepass la recherche dans le répertoire de travail.
Cette vulnérabilité peut donc exécuter du code arbitraire dans les conditions suivantes :

- la librairie dwmapi.dll modifiée (hostile) a été déposée dans le répertoire de KeePass ;
- l'exécution de KeePass se fait via le shell Windows avec comme répertoire courant celui où se trouve la librairie dwmapi.dll modifiée.

La mise à jour 2.13 de KeePass comble cette vulnérabilité.

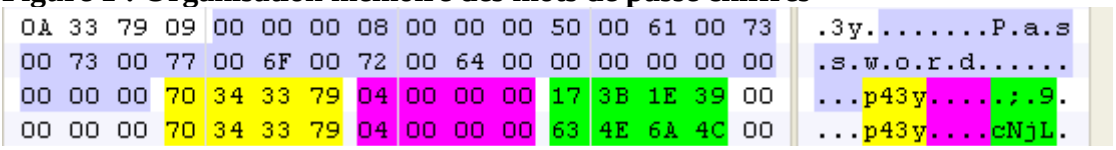
2.3.5.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Deux vulnérabilités ont été découvertes lors de l'évaluation. Elles concernent le mécanisme de protection des mots de passe et le mécanisme d'obfuscation du presse-papiers.

Vulnérabilité du mécanisme de protection des mots de passe en mémoire

Les mots de passe sont brouillés à l'aide d'un XOR avec la sortie d'une séquence pseudo-aléatoire. Le masque utilisé pour le XOR est stocké à coté du bloc d'octets brouillé.

Figure 1 : Organisation mémoire des mots de passe chiffrés



Dans la Figure 1, le motif à rechercher est le bloc bleu avec le mot « Password » en Unicode UTF-16. Ce motif est fixe. Les zones jaunes correspondent à l'identifiant d'un objet tableau d'octets (identifiant dynamique à chaque session). Les zones violettes codent à la taille de l'objet. Les zones vertes sont le mot de passe brouillé et le masque utilisé pour le XOR.
De plus, les zones mémoires ne sont pas marquées comme non déplaçables ce qui peut entraîner leur copie dans le fichier de pagination et faciliter la récupération des mots de passe après la fermeture du logiciel.

Avis d'expert
Le système de protection des mots de passe en mémoire ne protège que contre des attaques simples. Il est possible d'exploiter automatiquement les fichiers de pagination ou d'hibernation d'un ordinateur pour en extraire les mots de passe et les déchiffrer.

De plus, la non-déclaration des zones mémoires contenant des clefs temporaires comme zones non déplaçables peut introduire des non-conformités sur l'effacement de données temporaires si les contraintes mémoires sont trop fortes.

Cependant, les hypothèses d'environnement d'utilisation du produit couvrent cette dernière menace (cf. §2.3.6.2).

Vulnérabilité sur le mécanisme d'obfuscation du presse-papiers (TCATO)
L'évaluateur a développé un script permettant la capture des événements clavier ainsi que le contenu du presse-papier.

Avis d'expert
Le mécanisme TCATO implémenté dans KeePass offre une protection contre les logiciels n'implémentant que l'une de ces deux attaques.

On rappelle qu'une protection purement logicielle contre une attaque combinant la capture des événements clavier ainsi que le contenu du presse-papier n'est pas réaliste. Il est donc important de respecter les hypothèses d'environnement d'utilisation du produit pour s'en prémunir (cf. §2.3.6.2).

Vulnérabilité dans la journalisation des accès aux mots de passe
Il est possible de consulter un mot de passe sans provoquer de mise à jour du fichier de journalisation.

Avis d'expert
Cette vulnérabilité est non critique.

2.3.6 Analyse de la facilité d'emploi et préconisations

2.3.6.1 Cas où la sécurité est remise en cause
La sécurité de l'authentification et du chiffrement de la base est remise en cause lorsque l'utilisateur choisit un mot de passe ou un fichier clé de faible entropie.

2.3.6.2 Recommandations pour une utilisation sûre du produit
Il est recommandé d'utiliser la fonction de génération de mots de passe pour protéger l'accès à la base de données.
Le mécanisme TCATO n'est pas activé par défaut car il n'est pas compatible avec tous les mécanismes d'entrée de mots de passe (notamment ceux qui interdisent l'utilisation du presse-papier). Il est recommandé d'activer le mécanisme TCATO pour les applications le permettant.
Etant donné la présence de mots de passe déchiffrables dans le fichier de pagination ou le fichier d'hibernation, une mesure liée à la limitation de l'accès aux périphériques pouvant stocker ces fichiers doit être introduite.

2.3.6.3 Avis d'expert sur la facilité d'emploi

Le produit est simple à utiliser. L'interface est claire et bien documentée.

2.3.7 Accès aux développeurs

Le code source complet est disponible depuis le site de KeePass. L'évaluateur n'a pas eu de contact avec la communauté de développeurs de KeePass durant l'évaluation.

2.4 Analyse de la résistance des mécanismes cryptographiques

Chiffrement symétrique de la base de données
L'utilisation de l'algorithme symétrique AES en mode CBC est conforme au référentiel [RGS_B_1] de l'ANSSI.

Authentification à la base de données
L'utilisation de l'algorithme symétrique AES en mode ECB et CBC ainsi que l'algorithme de hachage SHA256 sont conformes au référentiel [RGS_B_1] de l'ANSSI.

2.5 Analyse du générateur d'aléas

Générateur aléatoire utilisé pour la génération des clés de chiffrement
Le générateur aléatoire utilisé pour la génération des clés de chiffrement est basé sur un retraitement algorithmique utilisant un état interne de 512 bits. L'architecture du retraitement algorithmique est conforme au référentiel [RGS_B_1] de l'ANSSI.

L'état interne est mis à jour à l'aide de la fonction de hachage SHA-512, les sorties du générateurs proviennent de sorties de la fonction de hachage SHA2. Le retraitement est conforme au référentiel [RGS_B_1] de l'ANSSI.

Le générateur d'aléa est conforme au référentiel [RGS_B_1] de l'ANSSI.

Générateur aléatoire utilisé dans la création de mots de passe
Le générateur de mots de passe basé sur Salsa20/10 est conforme au référentiel [RGS_B_1] de l'ANSSI.

Générateur aléatoire utilisé lors de la création d'un fichier clé
Ce générateur d'aléa consiste à brasser, par la fonction de hachage SHA-256, les données aléatoires déduites de mouvements de souris réalisés par l'utilisateur, avec les sorties du générateur aléatoire utilisé pour la génération de clés de chiffrement.

Ce dernier générateur est reconnu conforme au référentiel [RGS_B_1] de l'ANSSI. Par ailleurs, la fonction de hachage SHA-256 n'en altère pas les sorties. Le générateur d'aléa utilisé pour la création d'un fichier clé est donc lui aussi reconnu conforme au référentiel [RGS_B_1] de l'ANSSI.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce rapport de certification de sécurité de premier niveau atteste que le produit « KeePass Version 2.10 Portable » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

3.2 Restrictions d'usage

Dans le respect des hypothèses d'utilisation formulées par le développeur, aucune restriction d'usage n'est identifiée pour le produit KeePass Version 2.10 Portable.

Annexe 1. Références documentaires du produit évalué

[ST]	Cible de Sécurité CSPN KEEPASS v2.10 portable *Référence* : cible_CSPN_KEEPASS Version 2.1 *Date :* 08 Décembre 2010
[GUIDES]	Tutorial KeePass Version 2.0
[RTE]	Rapport d'évaluation CSPN. Projet. : KeePass *Référence* : KPS_CSPN Révision : 5.0 *Date :* 10/11/2010
[CRYPTO]	KeePass Spécification des mécanismes cryptographiques KEEPASS v2.10 portable *Référence* : spécifications_cryptographiques_CSPN_KEEPASS_2_1.doc *Date :* 11/08/2010

Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI, disponible sur www. ssi. gouv. fr
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2. 4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1. 4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1. 3. Documents disponibles sur www. ssi. gouv. fr
[RGS_B_1]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr