PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de certification
ANSSI-CSPN-2022/02

OpenStack Barbican

Version VICTORIA (11.0.1.dev10)

Paris, le 28 septembre 2022

Guillaume POUPARD
Le directeur général de l'Agence nationale
de la sécurité des systèmes d'information

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2022/02**
Nom du produit **OpenStack Barbican**
Référence/version du produit **Version VICTORIA (11.0.1.dev10)**
Catégorie de produit **Stockage sécurisé**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION** 51 boulevard de la Tour Maubourg 75700 Paris 07 SP
Développeur **THE OPENSTACK FOUNDATION**
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes
Fonctions de sécurité évaluées Contrôle d'accès Protection de la configuration Protection des secrets utilisateurs Protection des journaux
Fonctions de sécurité non évaluées Néant
Restriction(s) d'usage Oui (cf. §3.2)

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « OpenStack Barbican, Version VICTORIA » développé par THE OPENSTACK FOUNDATION.

OpenStack est un ensemble de logiciels libres qui permettent de créer et gérer des *clouds* privés ou publics à partir de *pools* de ressources virtuelles. Six de ces outils assurent les principaux services de *cloud computing* à savoir, le calcul, la mise en réseau, le stockage, la gestion des identités et la gestion des images.

Barbican correspond au service d'OpenStack (API REST) de stockage sécurisé, provisionnement et gestion des secrets (mots de passe, clés de chiffrement, certificats X.509). Ce système de gestion de clés est généralement utilisé pour mettre en place des mécanismes tels que la vérification de signature des images, le chiffrement de volumes, le chiffrement de disque éphémère, etc. Il permet de créer des secrets regroupés dans des conteneurs et attribués à un groupe d'utilisateurs, associés à des projets créés dans OpenStack.

Barbican a une architecture en *plugins* qui permettent de stocker des secrets dans un ou plusieurs magasins. Les magasins peuvent être de type logiciel (base SQL, …) ou physique (HSM).

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

☐	1	détection d'intrusions
☐	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	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	OpenStack Barbican
Numéro de la version évaluée	Version VICTORIA (11.0.1.dev10)

La version certifiée du produit peut être identifiée de la manière suivante :
- se connecter au *docker barbican_api* : `$ docker exec -it barbican_api /bin/bash` ;
- exécuter : `$ barbican-manage –version.`

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :
- le contrôle d'accès ;
- la protection de la configuration ;
- la protection des secrets utilisateurs ;
- la protection des journaux.

1.2.4 *Configuration évaluée*

L'évaluation porte sur le produit OpenStack Barbican utilisé avec :
- le *plugin* magasin de secrets « store_crypto » (stockage SQL) ;
- le *plugin* PKCS#11 utilisé afin de chiffrer les secrets et couplé avec un HSM Proteccio qui implémente l'interface Cryptoki PKCS#11.

La plateforme de tests est constituée des éléments suivants :
- un poste client *Kali Linux* utilisé pour faire les tests de robustesse et analyser les captures réalisées sur l'hôte openstack ;
- une machine Ubuntu 20.04.3 LTS, appelé « Hôte OpenStack », portant la cible et donc openstack utilisé pour réaliser les tests locaux, les captures et l'interception des flux du HSM ;
- un HSM « TrustWay Proteccio EL 1.05.03 » (considéré comme hors TOE) utilisé pour stocker les clés de chiffrement et de signature KEK.

Il s'agit d'une plateforme « *all in one* » car tous les conteneurs de services OpenStack son hébergés sur la même machine physique.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

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

L'installation a été réalisée avec l'outil *kolla-ansible* et en suivant les guides [GUIDES].

2.2.1.3 Notes et remarques diverses

Néant.

2.2.2 *Analyse de la documentation*

Dans le cadre de cette évaluation, l'évaluateur a eu accès à la documentation du produit [GUIDES] disponible sur le site officiel de l'éditeur.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'intégralité du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

Les risques identifiés lors de l'évaluation entraînent des recommandations d'usage pour l'utilisateur (voir chapitre 3.2).

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité n'ont pas été analysé car le produit repose sur le HSM pour réaliser les opérations cryptographiques. L'analyse a donc principalement consisté à vérifier la conformité des algorithmes cryptographiques utilisés par rapport au référentiel [ANSSI Crypto] et les appels au HSM que le produit effectue.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit ne comporte pas de générateur d'aléa entrant dans le périmètre d'évaluation.

3 La certification

3.1 Conclusion

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

Ce certificat atteste que le produit « OpenStack Barbican, Version VICTORIA (11.0.1.dev10) » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et suivre les recommandations et restrictions d'usage se trouvant dans les guides fournis [GUIDES], notamment :

- utiliser un HSM compatible qui supporte l'utilisation du mode GCM pour chiffrer les secrets utilisateurs. Sinon, utiliser le mode CBC et s'assurer d'une protection robuste (physique et logique) de la base de donnée de Barbican contre tout agent menaçant présent dans le réseau ou localement, afin d'assurer l'intégrité, mais aussi la confidentialité des secrets.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité CSPN - Produit OpenStack Barbican version « VICTORIA », référence CSPN-ST-OpenStack Barbican-1.06, version 1.06, 20 janvier 2022.
[RTE]	Rapports techniques d'évaluation : - Rapport Technique d'Evaluation CSPN - Produit Barbican - version 11.0.1.dev10, référence CSPN-RTE-BARBICANv11.0.1dev10-1.02, version 1.02, 20 janvier 2022 ; - Expertise des mécanismes cryptographiques - Produit Barbican - version 11.0.1.dev10, référence CSPN-CRY-Barbican v11.0.1dev10-1.01, version 1.01, 1 décembre 2021.
[GUIDES]	Guides d'utilisation, d'administration et d'installation du produit : - https://docs.openstack.org/barbican/victoria, consulté le 20 janvier 2022 ; - OPENSTACK – Procédure d'installation d'un environnement de test avec BARBICAN via KOLLA-ANSIBLE, référence 1132/ANSSI/SDE/DAT/BSS.

ANNEXE B. 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.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 3.0, 12 avril 2021. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.