PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2021/17

JPlatform 10

Version SP4 10.0.4 patch 20201210

Paris, le 1er septembre 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

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-2021/17**
Nom du produit **JPlatform 10**
Référence/version du produit **Version SP4 10.0.4 patch 20201210**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **JALIOS** 58 rue Pottier 78150 Le Chesnay, France
Développeur **JALIOS** 58 rue Pottier 78150 Le Chesnay, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Authentification locale des utilisateurs Gestion des droits sur les publications Gestion des droits sur les catégories Gestion des droits d'administration centrale Contrôle d'accès sur l'espace collaboratif Fonction d'audit Nettoyage des contributions par liste blanche Fonction de stockage sécurisé des *credentials* des applications tierces Gestion des workflows
Fonctions de sécurité non évaluées Néant
Restriction(s) d'usage Non

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 « JPlatform 10, Version SP4 10.0.4 patch 20201210 » développé par JALIOS.

Ce produit est destiné à être utilisé en entreprise pour créer une plateforme de travail numérique (*Digital Workplace*), d'intranet social et collaboratif ou encore de GED collaborative.

Pour cela, JPlatform 10 permet aux entreprises de mettre en œuvre au sein d'un portail unique les fonctionnalités suivantes :

- réseau social d'entreprise : espaces communautaires, profil riche déclaratif…
- espaces collaboratifs : blog, wiki, calendrier partagé, planification…
- portail d'entreprise et espace de travail personnalisé : intégration dans le SI, nombreux connecteurs, applications métiers…
- gestion électronique documentaire : partage documentaire et édition collaborative, recherche avancée, gestion des versions…
- *social learning* : catalogue de savoirs, création de parcours, partage de savoir-faire, tableaux de bord…
- gestion de contenu : espaces éditoriaux, *workflow* éditorial ou métier, gestion des droits…

La figure ci-dessous explicite l'architecture générale dans laquelle le produit s'inscrit.

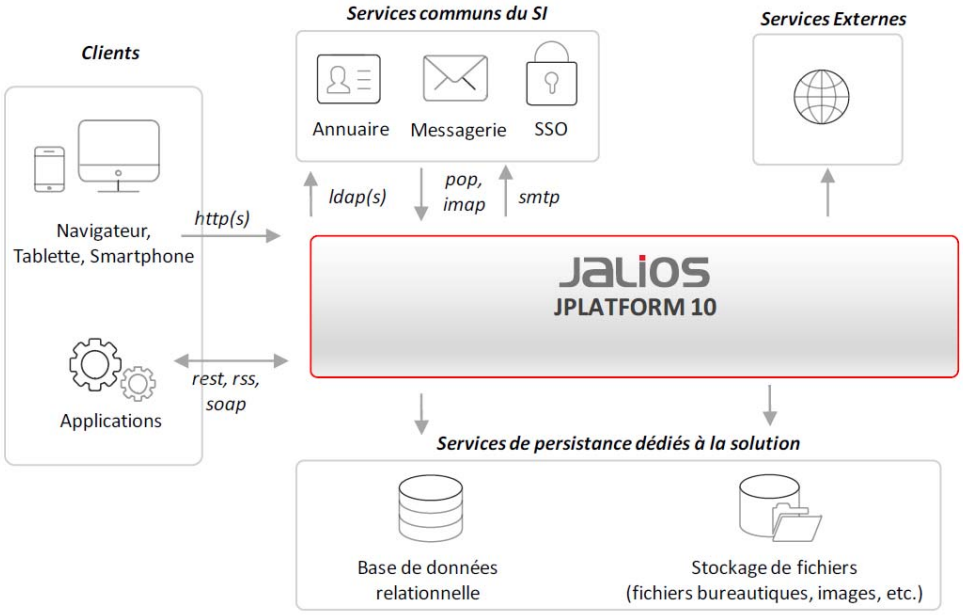

Figure 1 - Architecture Générale.

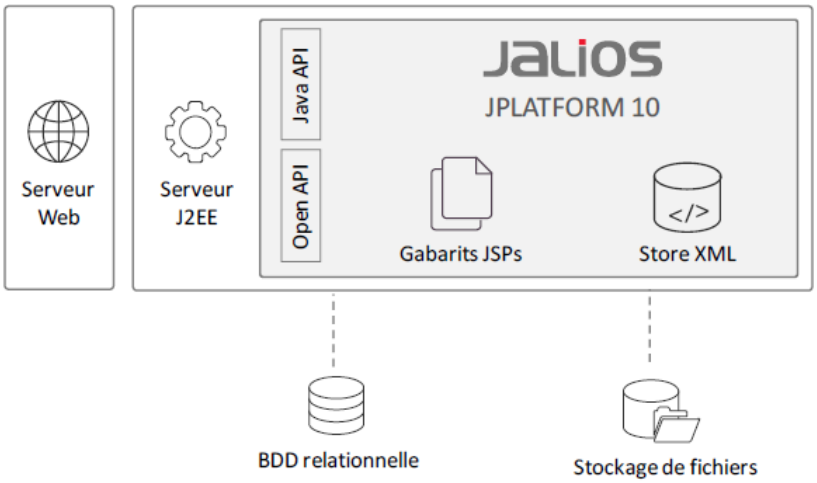

Figure 2 - Architecture Produit.

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	JPlatform 10
Numéro de la version évaluée	Version SP4 10.0.4 patch 20201210

La version certifiée du produit peut être identifiée en consultant la ressource « /admin/siteInfo.jsp » ou « état du site » depuis un compte administrateur.

La version du patch appliqué peut être consultée depuis : « /admin/displayPlugin.jsp?name=PatchPlugin ».

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'authentification locale des utilisateurs ;
- la gestion des droits sur les publications ;
- la gestion des droits sur les catégories ;
- la gestion des droits d'administration centrale ;
- le contrôle d'accès sur l'espace collaboratif ;
- la fonction d'audit ;
- le nettoyage des contributions par liste blanche ;
- la fonction de stockage sécurisée des *credentials* des applications tierces ;
- la gestion des *workflow*.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond :

- à la plateforme JPlatform en version SP4 10.0.4 avec le patch 20201210 ;
- à la JVM Java : OpenJDK 11 en version 11.0.9.1+1 ;
- au serveur applicatif JavaEE : Apache Tomcat en version 9.0.41.

Dans le cadre de la certification CSPN, le contexte d'emploi de JPLATFORM 10 se limite à une configuration particulière de la plateforme :

- site privé nécessitant une authentification ;
- deux langues de contribution : français et anglais ;
- utilisation de la base de données embarquée « Derby » ;
- serveur de mail configuré ;
- pas de proxy de sortie configuré ;
- OpenAPI activé.

Les fonctionnalités suivantes sont désactivées :

- LDAP ;
- WebDAV ;
- JSync ;
- Profil de consultation (« Audiencement ») ;
- Mail entrant.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en ANNEXE B.

2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3 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].

2.3.1 *Installation du produit*

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

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

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

L'installation se fait en suivant le guide du développeur [GUIDES].

2.3.1.3 Durée de l'installation

L'installation peut s'effectuer en une demi-journée.

2.3.1.4 Notes et remarques diverses

Néant.

2.3.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents d'installation et d'exploitation, consultables sur le site de JALIOS, dans le cadre de cette évaluation.

Le guide du produit permet d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

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

2.3.4 *Analyse de la conformité des fonctions de sécurité*

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

2.3.5 *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.

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

2.3.6.1 Liste des vulnérabilités connues

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

2.3.6.2 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 et dans le contexte défini par la cible de sécurité [CDS].

2.3.7 *Analyse de la facilité d'emploi*

2.3.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.7.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté.

2.3.7.3 Notes et remarques diverses

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

2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

2.5 Analyse du générateur d'aléas

Le produit utilise le générateur d'aléas SecureRandom de Java pour générer les sels servant au stockage des mots de passe.

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 « JPlatform 10, Version SP4 10.0.4 patch 20201210 » 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.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité CSPN JPLATFORM 10 Version : 1.4 ; Date : 4 janvier 2021.
[RTE]	Rapport Technique d'Évaluation CSPN Jalios-CSPN-2020 – JPlatform 10 SP4 Référence : OPPIDA/CESTI/Jalios-CSPN-2020/RTE/2.0 ; Version : 2.0 ; Date : 16 juin 2021.
[GUIDES]	JPLATFORM 10 Manuel d'installation et d'exploitation Version : 1.0.19 ; Date : 2021.

ANNEXE B. Références 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-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.