AFRICA UNIV

SECURITE ODOO

Normes, certifications et mesures de sécurité de la plateforme Odoo

Document de synthèse : Sécurité Cloud & Sécurité Applicative

support@africauniv.tech 690 36 35 77 RC/DLA/2023/B/7355 NUI: M032118528894U Douala,Cameroun

Table des matières

I. Sécurité des serveurs Cloud (Odoo.sh)

Odoo héberge ses environnements Cloud (Odoo Online et Odoo.sh) chez des fournisseurs d'infrastructure de premier plan (notamment OVHcloud et Google Cloud), et s'appuie sur un ensemble de normes et de certifications reconnues internationalement pour garantir la sécurité, la disponibilité et la confidentialité des données hébergées.

1. Certification ISO/IEC 27001 :2022

Depuis avril 2026, Odoo a obtenu la certification ISO/IEC 27001 :2022, la norme internationale de référence pour les Systèmes de Management de la Sécurité de l'Information (SMSI). Cette certification, validée par un audit tiers indépendant, couvre :

- La conception, le développement et le support du logiciel Odoo ;
- Les services professionnels d'implémentation ;
- L'hébergement Cloud (SaaS via Odoo Online et PaaS via Odoo.sh) ;
- Les services de plateforme de confiance, incluant l'échange électronique de documents avec les réseaux bancaires, les plateformes de commerce numérique et les administrations publiques (facturation électronique, Peppol, etc.).

Cette certification repose sur le triptyque CIA (Confidentiality, Integrity, Availability) : garantir que seules les personnes autorisées accèdent aux données, que ces données restent exactes et protégées contre toute modification non autorisée, et que les systèmes restent disponibles en permanence.

2. Rapports d'audit SOC 1 et SOC 2

Odoo maintient annuellement des rapports d'audit externes SOC (System and Organization Controls), réalisés par des auditeurs indépendants, couvrant à la fois Odoo Online (SaaS) et Odoo.sh (PaaS) :

- **SOC 1 (ISAE 3402) Type I & II :** axé sur les contrôles pertinents pour le reporting financier.
- **SOC 2 Type I & II :** évalue la conception (Type I) et l'efficacité opérationnelle (Type II) des contrôles de sécurité, de disponibilité et de confidentialité.

Le SOC 2 est particulièrement recherché par les entreprises clientes nord-américaines et européennes, tandis que l'ISO 27001 est davantage reconnu à l'international, notamment dans les procédures d'achat de grands groupes.

3. Auto-évaluation CAIQ (Cloud Security Alliance)

Odoo met à disposition une auto-évaluation CAIQ (Consensus Assessments Initiative Questionnaire, v3.1) de la Cloud Security Alliance, disponible sur sa page de politique de sécurité (odoo.com/security). Le CAIQ met en correspondance les contrôles d'Odoo avec plusieurs référentiels reconnus :

- ISO 27001
- PCI DSS (paiements par carte)
- FedRAMP (référentiel fédéral américain)
- HIPAA (données de santé, USA)
- HITRUST

4. Certifications des hébergeurs partenaires

Les données des clients Odoo sont hébergées dans des centres de données sécurisés et certifiés, opérés par des fournisseurs reconnus, en particulier OVHcloud et Google Cloud. Ces hébergeurs disposent eux-mêmes de certifications ISO 27001 et d'autres normes internationalement reconnues, ce qui renforce la chaîne de confiance de bout en bout (Odoo + infrastructure sous-jacente).

5. Conformité RGPD (Règlement Général sur la Protection des Données)

En tant qu'hébergeur Cloud opérant en Europe, Odoo intègre les exigences du RGPD dans ses pratiques :

- Localisation des environnements de production et des sauvegardes documentée par région d'hébergement, avec indication des pays situés dans l'UE ou bénéficiant d'une décision d'adéquation ;
- Mise à disposition d'outils permettant aux entreprises clientes de répondre aux droits des personnes concernées (accès, rectification, effacement, portabilité) ;
- Politique de confidentialité publique et régulièrement mise à jour (odoo.com/privacy) ;

  Rappel important : la conformité RGPD reste une responsabilité partagée, Odoo fournit les outils et l'infrastructure, mais chaque entreprise reste responsable du traitement de ses propres données et de la configuration adéquate de la plateforme.

6. Protection contre les attaques réseau (DDoS et intrusions)

L'infrastructure Cloud d'Odoo bénéficie des capacités de résilience de ses fournisseurs de centres de données :

- Grande capacité réseau conçue pour résister aux attaques par déni de service distribué (DDoS) ;
- Systèmes de mitigation automatiques et manuels détectant et détournant le trafic malveillant en périphérie de réseaux multicontinentaux ;
- Pare-feu et contre-mesures d'intrusion sur les serveurs Cloud, permettant de détecter et bloquer les attaques par force brute sur les mots de passe ;
- Possibilité, pour les administrateurs de bases de données clientes, de configurer une limitation de taux (rate limiting) et un délai de refroidissement en cas de tentatives de connexion répétées.

7. Autres référentiels évoqués (ISO 27017 / 27018 / 27034, OWASP ASVS)

Au-delà de l'ISO 27001, Odoo suit les meilleures pratiques du secteur et sélectionne des centres de données répondant à des exigences de sécurité minimales, en s'appuyant notamment sur les principes de l'OWASP Top 10 et de l'OWASP ASVS, intégrés aux processus de revue de code et de développement.

II. Sécurité applicative (le logiciel Odoo)

1. Sécurité du logiciel

Odoo est open source : son code source est constamment examiné par les utilisateurs et contributeurs du monde entier. Les rapports de bogues remontés par la communauté constituent une source importante de feedback en matière de sécurité. Les développeurs sont encouragés à auditer le code et à signaler les problèmes de sécurité identifiés.

Les processus de R&D d'Odoo intègrent des étapes de revue de code comportant un volet sécurité, aussi bien pour les nouveaux développements que pour les contributions externes.

2. Sécurité par conception (« Security by Design »)

Odoo est conçu de manière à éviter l'introduction des vulnérabilités de sécurité les plus courantes :

- **Injections SQL** : empêchées par l'utilisation d'une API de haut niveau (ORM) qui ne nécessite pas l'écriture manuelle de requêtes SQL.
- **Attaques XSS (Cross-Site Scripting)** : évitées grâce à un système de modélisation de haut niveau qui échappe automatiquement les données injectées dans les vues.
- **Accès RPC non autorisé** : le Framework empêche l'accès RPC aux méthodes privées, ce qui complique l'exploitation de vulnérabilités.

3. Audits de sécurité indépendants

Odoo fait régulièrement l'objet d'audits menés par des sociétés indépendantes mandatées par des clients et prospects (audits et tests d'intrusion). Les résultats sont transmis à l'équipe de sécurité d'Odoo, qui applique les mesures correctives nécessaires. Ces rapports restent confidentiels et ne sont pas divulgués publiquement.

Odoo bénéficie également d'une communauté active de chercheurs en sécurité indépendants qui surveillent en continu le code source, dans le cadre du programme de divulgation responsable d'Odoo.

4. Prévention des principales vulnérabilités OWASP

Odoo positionne sa sécurité applicative par rapport aux principales vulnérabilités recensées par l'OWASP (Open Web Application Security Project) :

a. Failles d'injection (dont injection SQL)

L'ORM d'Odoo abstrait la construction des requêtes : les développeurs ne rédigent pas de requêtes SQL manuelles, celles-ci sont générées par l'ORM avec des paramètres systématiquement échappés, empêchant par défaut les injections SQL.

b. Cross-Site Scripting (XSS)

Le Framework échappe par défaut toutes les expressions affichées dans les vues et pages web. Les développeurs doivent explicitement marquer une expression comme « sûre » pour qu'elle échappe à cet échappement automatique, ce qui limite fortement le risque de XSS.

c. Cross-Site Request Forgery (CSRF)

Le moteur de site web d'Odoo intègre un mécanisme de protection CSRF : aucun contrôleur HTTP ne peut recevoir de requête POST sans le jeton de sécurité correspondant, ce jeton n'étant connu que lorsque l'utilisateur a réellement accédé au formulaire concerné.

d. Exécution de fichier malveillant (RFI)

Odoo n'expose pas de fonctions permettant l'inclusion de fichiers à distance. Les expressions personnalisées que les utilisateurs privilégiés peuvent ajouter sont toujours évaluées dans un environnement sandbox limitant l'accès aux seules fonctions autorisées.

e. Référence directe non sécurisée à un objet

Le contrôle d'accès d'Odoo n'est pas implémenté au niveau de l'interface utilisateur : chaque requête doit systématiquement passer par la couche de validation d'accès aux données, ce qui empêche un attaquant de contourner ce contrôle en manipulant des références d'objets dans une URL.

f. Stockage cryptographique non sécurisé

Les mots de passe utilisateurs sont protégés par une fonction de hachage sécurisée standard (PBKDF2 / SHA512 par défaut, avec étirement de clé). Odoo permet également l'authentification via des systèmes externes (OAuth 2.0, LDAP) afin d'éviter le stockage local des mots de passe.

g. Communications non sécurisées

Odoo Cloud fonctionne en HTTPS par défaut. Pour les installations on-premise, il est recommandé de placer Odoo derrière un serveur web assurant le chiffrement (Apache, Lighttpd, nginx). Le guide d'implémentation d'Odoo fournit une checklist de sécurité pour les déploiements publics.

h. Défaillance dans la restriction des accès URL

Le contrôle d'accès ne repose jamais sur le simple masquage d'URLs : chaque requête passe par la couche de validation d'accès. Dans les rares cas où une URL sensible est nécessaire (ex. confirmation de commande client), celle-ci est signée numériquement avec un jeton unique et transmise uniquement au destinataire prévu.

5. Signalement des vulnérabilités

Toute vulnérabilité identifiée peut être signalée via la page de divulgation responsable d'Odoo. Ces signalements sont traités en haute priorité : le problème est immédiatement évalué et corrigé par l'équipe de sécurité d'Odoo, en collaboration avec le rapporteur, puis divulgué de manière responsable aux clients et utilisateurs concernés.

WEBOGRAPHIE

Sécurité générale / politique officielle Odoo

- https://www.odoo.com/security
- https://www.odoo.com/security/compliance-reports/iso27001/

Certification ISO 27001

- https://www.odoo.com/blog/odoo-news-5/your-data-secured-odoo-is-iso-27001-certified-2196

SOC 1 / SOC 2 / CAIQ (forum officiel Odoo)

- https://www.odoo.com/forum/help-1/is-odoo-soc-certified-or-compliant-what-about-is-27001-caiq-soc2-nis-2-206115
- https://www.odoo.com/forum/help-1/does-odoo-have-certificates-regarding-international-standards-isoiec-27001-isoiec-27002-isoiec-27017-isoiec-27018-isoiec-27034-owasp-top-10-and-asvs-190936

RGPD / Politique de confidentialité Odoo

- https://www.odoo.com/fr_FR/gdpr
- https://www.odoo.com/fr_FR/privacy

Hébergeurs partenaires (OVHcloud, RGPD)

- https://www.ovhcloud.com/fr/personal-data-protection/gdpr/
- https://www.ovhcloud.com/fr/personal-data-protection/security/
- https://www.ovhcloud.com/fr/personal-data-protection/