Nom doc. : **Sécurité d'Oxygis**

Version : 18/06/2025

Résumé : Votre sécurité est très importante pour nous ! Voici un résumé de ce que nous faisons chaque jour pour garantir que vos données sont en sécurité avec Oxygis et que nous appliquons les meilleures pratiques de sécurité sur notre version hébergée, le Cloud Oxygis.

1 - Oxygis Cloud (Infrastructure Cloud d'Oxygis)

I. Sauvegardes / reprise après sinistre

- Sauvegardes hebdomadaires conservées pendant 1 an
- Les sauvegardes sont conservées sur Microsoft Azure
- Les sauvegardes sont répliquées dans au moins 3 centres de données différents dans une zone de disponibilité en Europe Occidentale. Sur demande, des répliques automatiques peuvent être faites dans d'autres zones de disponibilité (ceci pourrait engendrer des frais supplémentaires, répercutés sur le Client).
- Vous pouvez contacter notre service d'assistance pour restaurer n'importe laquelle de ces sauvegardes sur votre base de données active (ou sur le côté).
- Les emplacements réels de nos centres de données sont précisés dans notre ***Politique de Confidentialité***.
- **Basculement matériel :** aucun service n'est hébergé directement sur du "baremetal", mais uniquement sur des serveurs virtuels ou des services gérés de Microsoft Azure ou Amazon Web Services.
- **Reprise après sinistre :** en cas de sinistre complet, avec un centre de données *entièrement hors service pendant une période prolongée,* empêchant le basculement vers notre hot-standby local (cela ne s'est jamais produit jusqu'à présent, c'est le plan le plus défavorable), nous avons les objectifs suivants :
    - **RPO** (Recovery Point Objective) = 24h. Cela signifie que vous pouvez perdre au maximum 24h de travail si les données ne peuvent pas être récupérées et que nous devons restaurer votre dernière sauvegarde quotidienne.
    - **RTO** (Recovery Time Objective) = 24h pour les abonnements payants, 48h pour les essais gratuits, les offres éducatives, les utilisateurs freemium, etc. Il s'agit du temps nécessaire pour restaurer le service dans un autre centre de données si une catastrophe se produit et qu'un centre de données est complètement hors service.
    - Comment cela est-il réalisé : nous surveillons activement nos sauvegardes quotidiennes, et elles sont répliquées en de multiples centres de données dans une zone de disponibilité. Nous disposons d'un système d'approvisionnement automatisé pour déployer nos services dans un nouveau site d'hébergement. La

restauration des données basée sur nos sauvegardes de la veille peut alors être effectuée en quelques heures (pour les clusters les plus importants).

II. Sécurité des bases de données

- Les données des Clients peuvent être stockées dans une base de données dédiée - aucun partage de données entre les Clients.

III. Sécurité du mot de passe

- Les mots de passe des Clients sont protégés par un cryptage PBKDF2+SHA512 conforme aux normes industrielles (salés + étirés pendant des milliers de tours).
- Le personnel d'Oxygis n'a pas accès à votre mot de passe et ne peut pas le récupérer pour vous, la seule option si vous le perdez est de le réinitialiser.
- Les identifiants de connexion sont toujours transmis de manière sécurisée via HTTPS.
- Politiques de mot de passe : les mots de passe doivent avoir une taille minimum de 10 caractères et doivent contenir au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

IV. Accès du personnel

- Le personnel du service d'assistance d'Oxygis peut se connecter à votre compte pour accéder aux paramètres liés à votre problème d'assistance. Pour cela, ils utilisent leurs propres informations d'identification, et non votre mot de passe (qu'ils n'ont aucun moyen de connaître).
- Cet accès spécial du personnel améliore l'efficacité et la sécurité : il peut immédiatement reproduire le problème que vous rencontrez, vous ne devez jamais partager votre mot de passe, et nous pouvons auditer et contrôler les actions du personnel séparément !
- Le personnel de notre service d'assistance s'efforce de respecter au maximum votre vie privée et n'accède qu'aux fichiers et paramètres nécessaires pour diagnostiquer et résoudre votre problème.

V. Sécurité physique

Les serveurs Oxygis Cloud sont hébergés sur Microsoft Azure, aucun accès physique n’est possible

VI. Communications

- Toutes les communications de données vers les instances Clientes sont protégées par un cryptage SSL 256 bits (HTTPS) de pointe.

2 - Oxygis (le logiciel)

I. Sécurité des logiciels

Oxygis est codé en C# pour le backend et en AngularJS pour le front-end.

Les processus de R&D d'Oxygis prévoient des étapes de révision du code qui incluent les aspects de sécurité des nouveaux éléments de code ainsi que les éléments existants.

II. Sécurité dès la conception

Oxygis est conçu de manière à éviter l'introduction des failles de sécurité les plus courantes :

- Les injections SQL sont évitées grâce à l'utilisation d'une API de niveau supérieur qui ne nécessite pas de requêtes SQL manuelles.
- Les attaques XSS sont évitées grâce à l'utilisation d'un système de modélisation de haut niveau qui échappe automatiquement aux données injectées.

Consultez également la section **Top Vulnérabilités de l'OWASP** pour voir comment Oxygis est conçu dès le départ pour empêcher l'apparition de telles vulnérabilités.

III. Top des vulnérabilités de l'OWASP

Voici la position d'Oxygis sur les principaux problèmes de sécurité des applications Web, tels que répertoriés par l'**Open Web Application Security Project** (OWASP) :

- **Failles d'injection :** Les failles d'injection, notamment l'injection SQL, sont courantes dans les applications Web. L'injection se produit lorsque des données fournies par l'utilisateur sont envoyées à un interpréteur dans le cadre d'une commande ou d'une requête. Les données hostiles de l'attaquant incitent l'interpréteur à exécuter des commandes non souhaitées ou à modifier des données.

  Oxygis utilise un ORM qui abstrait la construction des requêtes et empêche les injections SQL. Normalement, les développeurs n'élaborent pas manuellement les requêtes SQL, qui sont générées par l'ORM, et les paramètres sont toujours correctement échappés.

- **Cross Site Scripting (XSS) :** Les failles XSS se produisent lorsqu'une application prend des données fournies par l'utilisateur et les envoie à un navigateur Web sans valider ou coder ce contenu au préalable. XSS permet aux attaquants d'exécuter des scripts dans le

navigateur de la victime, ce qui peut détourner des sessions d'utilisateurs, défigurer des sites web, éventuellement introduire des vers, etc.

Oxygis échappe toutes les données ce qui empêche les XSS.

- **Cross Site Request Forgery (CSRF) :** Une attaque CSRF force le navigateur d'une victime connectée à envoyer une fausse requête HTTP, incluant le cookie de session de la victime et toute autre information d'authentification incluse automatiquement, à une application web vulnérable. Cela permet à l'attaquant de forcer le navigateur de la victime à générer des requêtes que l'application vulnérable pense être des requêtes légitimes de la victime.

  Oxygis comprend un mécanisme de protection CSRF intégré. Il empêche tout contrôleur HTTP de recevoir une requête sans le jeton de sécurité correspondant. Il s'agit de la technique recommandée pour la prévention CSRF.

- **Exécution de fichiers malveillants :** Le code vulnérable à l'inclusion de fichiers à distance (RFI) permet aux attaquants d'inclure du code et des données hostiles, ce qui entraîne des attaques dévastatrices, comme la compromission totale du serveur.

  Oxygis n'expose pas de fonctions permettant d'effectuer des inclusions de fichiers à distance.

- **Référence directe à un objet non sécurisée :** Une référence directe à un objet se produit lorsqu'un développeur expose une référence à un objet de mise en œuvre interne, tel qu'un fichier, un répertoire, un enregistrement de base de données ou une clé, sous forme d'URL ou de paramètre de formulaire. Les attaquants peuvent manipuler ces références pour accéder à d'autres objets sans autorisation.

  Le contrôle d'accès à Oxygis n'est pas mis en œuvre au niveau de l'interface utilisateur, il n'y a donc aucun risque à exposer des références à des objets internes dans les URL. Les attaquants ne peuvent pas contourner la couche de contrôle d'accès en manipulant ces références, car chaque requête doit toujours passer par la couche de validation de l'accès aux données.

- **Stockage cryptographique non sécurisé :** Les applications Web utilisent rarement les fonctions cryptographiques de manière appropriée pour protéger les données et les informations d'identification. Les attaquants utilisent des données faiblement protégées pour commettre des usurpations d'identité et d'autres délits, comme la fraude à la carte de crédit.

  Oxygis utilise un hachage sécurisé standard pour les mots de passe des utilisateurs (par défaut PKFDB2 + SHA-512, avec étirement de la clé) pour protéger les mots de passe stockés. Il est également possible d'utiliser des systèmes d'authentification externes afin d'éviter tout stockage local des mots de passe des utilisateurs.

- **Communications non sécurisées :** Les applications omettent souvent de crypter le trafic réseau lorsqu'il est nécessaire de protéger des communications sensibles.

  Oxygis fonctionne avec HTTPS.

- **Absence de restriction de l'accès aux URL :** Souvent, une application ne protège les fonctionnalités sensibles qu'en empêchant l'affichage de liens ou d'URL aux utilisateurs non autorisés. Les attaquants peuvent utiliser cette faiblesse pour accéder et effectuer des opérations non autorisées en accédant directement à ces URL.

  Le contrôle d'accès d'Oxygis n'est pas mis en œuvre au niveau de l'interface utilisateur, et la sécurité ne repose pas sur la dissimulation d'URL spéciales. Les attaquants ne peuvent pas contourner la couche de contrôle d'accès en réutilisant ou en manipulant une URL, car chaque demande doit passer par la couche de validation de l'accès aux données. Dans les rares cas où une URL fournit un accès non authentifié à des données sensibles, comme les URL spéciales que les Clients utilisent pour confirmer une commande, ces URL sont signées numériquement avec des jetons uniques et envoyées uniquement par courrier électronique au destinataire prévu.

IV. Signaler les vulnérabilités de sécurité

Si vous devez signaler une vulnérabilité de sécurité, veuillez en faire part à notre service d'assistance dès que possible. Ces rapports sont traités en haute priorité, le problème est immédiatement évalué et résolu par l'équipe de sécurité d'Oxygis, en collaboration avec le rapporteur, puis divulgué de manière responsable aux Clients et utilisateurs d'Oxygis.

Mise à jour et contact

Ce document est mis à jour régulièrement pour refléter l'évolution de nos pratiques de sécurité. Si vous avez des questions ou souhaitez en savoir plus, contactez-nous à info@oxygis.eu.

Documents connexes

- Politique de confidentialité
- Politique de divulgation responsable
- Contrat de niveau de service (SLA)
- Contrat d'abonnement

Compléments sur la sécurité

L'infrastructure cloud utilisée par Oxygis repose sur des centres de données Microsoft Azure certifiés ISO 27001, SOC 2 et conformes aux normes de sécurité de l'industrie. Les accès aux environnements de production sont strictement limités aux membres autorisés de l'équipe technique, tous soumis à un accord de confidentialité interne. Des journaux d'accès (logs) sont conservés pour analyse en cas d'incident.

Tests de sécurité

Oxygis réalise des tests de sécurité réguliers, notamment des scans automatisés de vulnérabilités sur ses environnements de production, afin de garantir une exposition minimale aux risques connus.

Authentification et gestion des accès

Oxygis recommande l'utilisation de mots de passe forts et d'une authentification à double facteur (2FA) pour l'accès à ses plateformes, lorsque disponible. Les rôles utilisateurs permettent une gestion fine des droits d'accès aux fonctionnalités et données.