Nom doc. :	**Oxygis - Divulgation responsable des vulnérabilités de sécurité**
Version mise à jour le :	18/06/2025
Résumé :	Aidez-nous à assurer la sécurité d'Oxygis

Politique de divulgation responsable

La sécurité des systèmes Oxygis est très importante pour nous, et nous considérons les problèmes de sécurité avec la plus haute priorité. Nous faisons de notre mieux chaque jour pour protéger les utilisateurs d'Oxygis des menaces de sécurité connues, et nous accueillons tous les rapports de vulnérabilité de sécurité découverts par nos utilisateurs et contributeurs.

Nous nous engageons à traiter les rapports de vulnérabilité avec la plus grande attention, à condition que les règles suivantes soient respectées.

I. Signaler un problème

Veuillez partager en privé les détails de votre vulnérabilité de sécurité en envoyant un courriel à notre équipe de sécurité à info@oxygis.eu . Veillez à inclure le plus d'informations possible, notamment les étapes détaillées de la reproduction du problème, les versions concernées, les résultats attendus et les résultats réels, ainsi que toute autre information susceptible de nous aider à réagir plus rapidement et plus efficacement. Nous avons tendance à préférer les **descriptions de bugs sous forme de texte accompagnées d'un script/exploit de preuve de concept,** plutôt que de longues vidéos.
Le signalement de vulnérabilités via des sites Web tiers n'est pas acceptable, à l'exception de l'utilisation de https://drop.aloalto.com pour le partage de mots de passe, car il enfreint les termes de notre politique.

Veuillez noter : nous recevons une majorité de rapports de sécurité qui ont peu ou pas d'impact sur la sécurité d'Oxygis et nous devons finalement les rejeter. Pour éviter une expérience décevante lorsque vous nous contactez, essayez de mettre en place une **attaque de type "proof-of-concept"** et examinez d'un œil critique **ce qui est réellement à risque**. Si le scénario d'attaque proposé s'avère **irréaliste**, votre rapport sera probablement rejeté. Veillez également à consulter la liste des **problèmes non admissibles** ci-dessous.

Vous pouvez envoyer ce rapport à partir d'un compte de messagerie anonyme, mais nous nous engageons à ne pas divulguer votre identité si vous ne le souhaitez pas.

Vous pouvez également utiliser https://drop.aloalto.com pour partager des informations critiques (par exemple : clés API, mots de passe, ...).

II. Procédure de réponse aux incidents

A. Procédure

- Vous pouvez partager les détails de la faille de sécurité avec notre équipe de sécurité en signalant un problème (voir ci-dessus).
- Nous accusons réception de votre demande et vérifions la vulnérabilité. Notre première réponse arrive généralement sous 48h.
- Si la vulnérabilité est valide et dans le champ d'application, nous travaillons à une correction en collaboration avec vous.
- Nous rédigeons un avis de sécurité détaillé décrivant le problème, ses impacts, les solutions de contournement possibles et la solution, et nous vous demandons de l'examiner.
- Nous avons diffusé en privé l'avis de sécurité et la correction aux parties prenantes et aux Clients avec un contrat d'Abonnement Oxygis.
- Nous accordons aux parties prenantes et aux Clients un délai raisonnable pour appliquer la correction, avant de la divulguer publiquement (par exemple, 2 à 3 semaines).
- Nous divulguons et diffusons l'avis de sécurité et la correction sur **nos chaînes publiques**.

B. Règles

Nous vous demandons de respecter les règles suivantes à tout moment :

- Testez exclusivement les vulnérabilités sur vos propres déploiements, sur demo.oxygis.eu, ou sur vos propres instances d'essai d'Oxygis Cloud.
- Ne tentez jamais d'accéder ou de modifier des données qui ne vous appartiennent pas.
- Ne tentez jamais d'exécuter des attaques par déni de service ou de compromettre la fiabilité et l'intégrité de services qui ne vous appartiennent pas.
- N'utilisez pas de scanners ou d'outils automatisés pour trouver des vulnérabilités, car leurs effets pourraient violer les règles précédentes (à moins que vous puissiez garantir qu'ils seront limités à moins de 5 requêtes/seconde et qu'ils ne violeront aucune autre règle).
- Ne tentez jamais d'attaques non-techniques, telles que l'ingénierie sociale, le hameçonnage ou les attaques physiques, contre qui que ce soit ou contre un système.
- Ne divulguez pas publiquement les vulnérabilités sans notre accord préalable (voir également la procédure de divulgation ci-dessus). Pendant la période de non-divulgation, vous êtes autorisé à utiliser/tester toute correction que nous avons fournie, à condition de ne pas mettre l'accent sur cette correction et de ne pas la

publier sous la forme d'un rapport de sécurité (c'est-à-dire que vous pouvez l'utiliser sur des serveurs de production).

C. En retour :

- Dans le cadre d'un test respectant les règles énoncées ci-dessus et n'occasionnant aucun préjudice réel, Oxygis s'engage à ne pas engager de poursuites civiles ou pénales à l'encontre du rapporteur.Nous traiterons votre rapport et vous répondrons dans les meilleurs délais.
- Nous fournirons un correctif dès que possible
- Nous travaillerons avec diligence avec les parties prenantes et les Clients afin de les aider à rétablir la sécurité de leurs systèmes.
- Nous ne divulguerons pas publiquement votre identité si vous ne souhaitez pas être crédité pour votre découverte.
- Cette politique ne constitue pas un programme de bug bounty. Aucun paiement n'est prévu en contrepartie des rapports.

III. Que signaler ?

Les vulnérabilités qualifiantes - À SIGNALER !

- Vecteurs d'injection SQL dans les méthodes des API publiques
- Les vulnérabilités XSS fonctionnent dans les navigateurs pris en charge
- Une authentification ou une gestion de session défaillante, permettant un accès non autorisé.

Vulnérabilités non qualifiantes - NE PAS SIGNALER !

- Les vulnérabilités XSS ne fonctionnent que dans les navigateurs non pris en charge ou dépréciés, ou nécessitent des paramètres de sécurité moins stricts.
- Attaques auto-XSS nécessitant que l'utilisateur copie/colle activement du code malveillant dans la fenêtre de son propre navigateur.
- Les "attaques XSS" par les administrateurs, par exemple via le téléchargement de fichiers (SVG, HTML, JS, ...) ou l'injection de scripts. Les administrateurs sont des webmasters, les restrictions de sécurité ne s'appliquent pas à eux, il s'agit d'une fonctionnalité.
- Limitation de la vitesse / Force brute / Scripting des composants fonctionnant comme prévu (ex : l'authentification du mot de passe, la réinitialisation du mot de passe, etc.)
- Recensement des utilisateurs (possibilité de vérifier qu'un nom d'utilisateur existe). Ne comporte pas beaucoup de risques et ne peut être évitée sans détériorer l'expérience de l'utilisateur.
- Les divulgations de chemins de fichiers, qui ne comportent pas de risque significatif et ne permettent pas des attaques qui seraient autrement impossibles.

- Les attaques de type "clickjacking" ou "phishing", qui utilisent des astuces d'ingénierie sociale pour abuser les utilisateurs, le système fonctionnant comme prévu.
- Tabnapping ou autres attaques de phishing menées en naviguant dans d'autres onglets du navigateur
- CSRF de déconnexion (pas d'attaque plausible + ne peut être empêché, par exemple via le jet de cookies ou le débordement de la boîte à cookies)
- Les téléchargements de fichiers réfléchis, une autre technique d'attaque qui nécessite une ingénierie sociale et n'est pas très pratique.
- Fuite de référents (y compris des jetons sensibles) via des liens de médias sociaux ou des demandes de publicité/analyse - très peu susceptibles d'être cliqués, ou d'être exploités pendant la période de validité par ces entreprises grand public !
- Plus généralement, les attaques reposant sur des techniques d'ingénierie physique ou sociale seront généralement rejetées.
- Déni de service (DoS) non permanent et DoS distribué (DDoS) qui maintiennent l'épuisement des ressources (cpu/réseau/mémoire) via un flux soutenu de requêtes/paquets.
- Politiques en matière de mots de passe (longueur, format, classes de caractères, etc.)
- Vérification manquante ou partielle des adresses électroniques
- La divulgation d'informations publiques ou d'informations ne comportant pas de risques significatifs (la liste des répertoires sur notre archive de téléchargements est une caractéristique obligatoire ! ;-))
- Politiques et systèmes de lutte contre le spam, tels que DKIM, SPF ou DMARC.
- Absence d'en-têtes HTTP Strict Transport Security (HSTS), de préchargement HSTS et de politiques HSTS.
- Scénarios d'attaque incluant une prise de contrôle des comptes de messagerie des utilisateurs

Si vous avez le moindre doute, demandez-nous d'abord !

Oxygis se réserve le droit de coordonner la divulgation publique d'une vulnérabilité en collaboration avec les chercheurs impliqués et les parties concernées (clients, partenaires, autorités compétentes), afin de garantir une correction préalable. La divulgation publique prématurée sans concertation pourrait compromettre cette approche et pourrait être exclue du champ de protection défini dans cette politique.