Doc. naam : **Oxygis - Verantwoordelijk onthullen van beveiligingsproblemen**

Versie bijgewerkt op :18/06/2025

Samenvatting : Help ons Oxygis veilig te houden

Beleid verantwoordelijke openbaarmaking

De veiligheid van Oxygis-systemen is erg belangrijk voor ons en we behandelen veiligheidskwesties met de hoogste prioriteit. We doen elke dag ons best om Oxygis gebruikers te beschermen tegen bekende veiligheidsbedreigingen en we verwelkomen alle meldingen van veiligheidslekken die ontdekt zijn door onze gebruikers en medewerkers.

We verbinden ons ertoe om meldingen van kwetsbaarheid met de grootste zorg te behandelen, op voorwaarde dat de volgende regels worden nageleefd.

I. Een probleem melden

Deel de details van uw beveiligingslek met ons door een e-mail te sturen naar ons beveiligingsteam opinfo@oxygis.eu . Zorg ervoor dat u zoveel mogelijk informatie verstrekt, waaronder de gedetailleerde stappen die nodig zijn om het probleem te reproduceren, de getroffen versies, de verwachte en werkelijke resultaten en alle andere informatie die ons kan helpen om sneller en effectiever te reageren. We geven de voorkeur aan **op tekst gebaseerde bugbeschrijvingen vergezeld van een proof-of-concept script/exploit,** in plaats van lange video's.
Het melden van kwetsbaarheden via websites van derden is niet acceptabel, met uitzondering van het gebruik van https://drop.aloalto.com voor het delen van wachtwoorden, aangezien dit in strijd is met de voorwaarden van ons beleid.

Let op: we ontvangen de meeste beveiligingsrapporten die weinig of geen invloed hebben op de beveiliging van Oxygis en we moeten ze uiteindelijk afwijzen. Om een teleurstellende ervaring te voorkomen wanneer u contact met ons opneemt, kunt u proberen een **"proof-of-concept" aanval** uit te voeren en kritisch te onderzoeken **wat er werkelijk in gevaar is**. Als het voorgestelde aanvalsscenario **onrealistisch** blijkt, wordt uw rapport waarschijnlijk afgewezen. Raadpleeg ook de onderstaande lijst met **problemen die niet in aanmerking komen**.

Je kunt dit rapport versturen vanaf een anoniem e-mailaccount, maar we verplichten ons om je identiteit niet bekend te maken als je dat niet wilt.

Je kunt ook https://drop.aloalto.com gebruiken om kritieke informatie te delen (zoals API-sleutels, wachtwoorden, enz.).

II. Procedure voor respons bij incidenten

A. Procedure

- Je kunt de details van het beveiligingslek met ons beveiligingsteam delen door een probleem te melden (zie hierboven).
- We bevestigen de ontvangst van je verzoek en controleren op kwetsbaarheid. Onze eerste reactie komt meestal binnen 48 uur.
- Als de kwetsbaarheid geldig is en binnen het toepassingsgebied valt, werken we met je samen om de kwetsbaarheid te verhelpen.
- We stellen een gedetailleerde veiligheidsmelding op met een beschrijving van het probleem, de impact ervan, mogelijke oplossingen en de oplossing, en vragen je om deze te bekijken.
- We hebben de beveiligingskennisgeving en de correctie persoonlijk verspreid onder belanghebbenden en klanten met een Oxygis Abonnementscontract.
- We geven belanghebbenden en klanten een redelijke periode om de correctie toe te passen, voordat we deze openbaar maken (bijvoorbeeld 2 tot 3 weken).
- We maken de veiligheidsmededeling en -correctie bekend en zenden deze uit op **onze openbare kanalen**.

B. Regels

We vragen je om de volgende regels te allen tijde te respecteren:

- Test kwetsbaarheden uitsluitend op uw eigen implementaties, op demo.oxygis.eu of op uw eigen testinstanties van Oxygis Cloud.
- Probeer nooit gegevens te openen of te wijzigen die niet van jou zijn.
- Probeer nooit denial-of-service-aanvallen uit te voeren of de betrouwbaarheid en integriteit van diensten die niet van jou zijn in gevaar te brengen.
- Gebruik geen scanners of geautomatiseerde tools om kwetsbaarheden te vinden, aangezien hun effecten de bovenstaande regels kunnen schenden (tenzij je kunt garanderen dat ze beperkt blijven tot minder dan 5 verzoeken/seconde en dat ze geen andere regels zullen schenden).
- Probeer nooit niet-technische aanvallen, zoals social engineering, phishing of fysieke aanvallen, uit te voeren op iemand of een systeem.
- Maak kwetsbaarheden niet openbaar zonder onze voorafgaande toestemming (zie ook bovenstaande openbaarmakingsprocedure). Tijdens de niet-openbaarmakingsperiode mag u een door ons geleverde fix gebruiken/testen, op voorwaarde dat u de fix niet benadrukt en deze niet publiceert als een beveiligingsrapport (d.w.z. dat u deze kunt gebruiken op productieservers).

C. In ruil :

- In het geval van een test die voldoet aan de hierboven uiteengezette regels en geen echte schade veroorzaakt, verbindt Oxygis zich ertoe geen burgerlijke of strafrechtelijke procedure tegen de melder op te starten. We zullen uw melding verwerken en u zo snel mogelijk antwoorden.
- We zorgen zo snel mogelijk voor een oplossing
- We zullen nauw samenwerken met belanghebbenden en klanten om hen te helpen de beveiliging van hun systemen te herstellen.
- We zullen uw identiteit niet publiekelijk bekendmaken als u niet gecrediteerd wilt worden voor uw ontdekking.
- Dit beleid is geen bug bounty programma. Er wordt niet betaald voor meldingen.

III. Wat te melden

Kwetsbaarheden - RAPPORT!

- SQL-injectievectoren in openbare API-methodes
- XSS-kwetsbaarheden werken in ondersteunde browsers
- Foutieve authenticatie of sessiebeheer, waardoor onbevoegden toegang krijgen.

Kwetsbaarheden die niet in aanmerking komen - NIET RAPPORTEREN!

- XSS-kwetsbaarheden werken alleen in niet-ondersteunde of verouderde browsers of vereisen minder strenge beveiligingsinstellingen.
- Auto-XSS-aanvallen waarbij de gebruiker actief kwaadaardige code moet kopiëren/plakken in zijn eigen browservenster.
- XSS-aanvallen" door beheerders, bijvoorbeeld door bestanden (SVG, HTML, JS, enz.) te downloaden of scripts te injecteren. Beheerders zijn webmasters, de beveiligingsbeperkingen zijn niet op hen van toepassing, dit is een functie.
- Snelheidsbeperking / brute kracht / scripting van onderdelen die werken zoals verwacht (bijv. wachtwoordverificatie, wachtwoord resetten, enz.)
- Gebruikersregistratie (mogelijkheid om te controleren of een gebruikersnaam bestaat). Niet erg riskant en kan niet worden vermeden zonder de gebruikerservaring te schaden.
- Openbaarmaking van bestandspaden, die geen significant risico met zich meebrengen en geen aanvallen mogelijk maken die anders onmogelijk zouden zijn.
- Clickjacking" of "phishing" aanvallen, waarbij social engineering trucs worden gebruikt om gebruikers te misleiden zodat het systeem werkt zoals bedoeld.
- Tabnapping of andere phishingaanvallen uitgevoerd tijdens het browsen in andere browsertabbladen
- CSRF-ontkoppeling (geen plausibele aanval + kan niet worden voorkomen, bijv. door cookies te gooien of de cookiebox te laten overlopen)
- Reflexieve bestandsdownloads, een andere aanvalstechniek die social engineering vereist en niet erg praktisch is.

Partners SRL
België : Eikelenbergstraat, 20, 1700 Dilbeek - België- Tel: +32 (0)2 736 10 17 - BTW : BE 0872.350.989
Frankrijk : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - BTW: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

- Lekken van verwijzers (inclusief gevoelige tokens) via links in sociale media of reclame-/analyseverzoeken - het is zeer onwaarschijnlijk dat er op wordt geklikt of dat er misbruik van wordt gemaakt tijdens de geldigheidsperiode door deze mainstreambedrijven!
- Meer in het algemeen zullen aanvallen gebaseerd op fysieke of social engineering technieken worden afgewezen.
- Niet-permanente Denial of Service (DoS) en Distributed DoS (DDoS) die bronnen (cpu/netwerk/geheugen) uitgeput houden via een aanhoudende stroom verzoeken/pakketten.
- Wachtwoordbeleid (lengte, formaat, tekenklassen, enz.)
- Ontbrekende of gedeeltelijke verificatie van e-mailadressen
- Openbaarmaking van openbare informatie of informatie die geen aanzienlijk risico met zich meebrengt (de lijst met directories in ons downloadarchief is een verplicht onderdeel! ;-))
- Antispambeleid en -systemen, zoals DKIM, SPF of DMARC.
- Afwezigheid van HTTP Strict Transport Security (HSTS)-headers, HSTS-preloading en HSTS-beleid.
- Aanvalscenario's waaronder het overnemen van e-mailaccounts van gebruikers

Als je twijfelt, vraag het ons dan eerst!

Oxygis behoudt zich het recht voor om de openbaarmaking van een kwetsbaarheid te coördineren in samenwerking met de betrokken onderzoekers en de betrokken partijen (klanten, partners, bevoegde autoriteiten), om een voorafgaande correctie te garanderen. Voortijdige openbaarmaking zonder overleg kan deze aanpak in gevaar brengen en kan worden uitgesloten van de beschermingsomvang die in dit beleid is gedefinieerd.

Partners SRL
België : Eikelenbergstraat, 20, 1700 Dilbeek - België- Tel: +32 (0)2 736 10 17 - BTW : BE 0872.350.989
Frankrijk : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - BTW: FR 13 811593730
www.oxygis.eu - info@oxygis.eu