Doc. name : **Oxygis - Responsible disclosure of security vulnerabilities**

Version updated on : 18/06/2025

Summary : Help us keep Oxygis safe

Responsible disclosure policy

The security of Oxygis systems is very important to us, and we treat security issues with the highest priority. We do our best every day to protect Oxygis users from known security threats, and we welcome all reports of security vulnerabilities discovered by our users and contributors.

We undertake to treat reports of vulnerability with the utmost care, provided that the following rules are complied with.

I. Report a problem

Please share the details of your security vulnerability privately by emailing our security team atinfo@oxygis.eu . Be sure to include as much information as possible, including the detailed steps involved in reproducing the problem, the versions affected, the expected and actual results, and any other information that might help us respond more quickly and effectively. We tend to prefer **text-based bug descriptions accompanied by a proof-of-concept script/exploit,** rather than long videos.
Vulnerability reporting via third-party websites is not acceptable, with the exception of the use of https://drop.aloalto.com for password sharing, as it breaches the terms of our policy.

Please note: we receive a majority of security reports that have little or no impact on the security of Oxygis and we ultimately have to reject them. To avoid a disappointing experience when you contact us, try to implement a **"proof-of-concept" attack** and critically examine **what is really at risk**. If the proposed attack scenario proves **unrealistic**, your report will probably be rejected. You should also consult the list of **ineligible problems** below.

You can send this report from an anonymous e-mail account, but we undertake not to disclose your identity if you do not wish to do so.

You can also use https://drop.aloalto.com to share critical information (e.g. API keys, passwords, etc.).

II. Incident response procedure

A. Procedure

- You can share details of the security breach with our security team by reporting a problem (see above).
- We acknowledge receipt of your request and check for vulnerability. Our first response usually arrives within 48 hours.
- If the vulnerability is valid and within the scope of application, we will work with you to correct it.
- We draw up a detailed safety notice describing the problem, its impact, possible workarounds and the solution, and ask you to review it.
- We have privately distributed the security notice and the correction to stakeholders and Customers with an Oxygis Subscription contract.
- We allow stakeholders and Customers a reasonable period of time to apply the correction, before disclosing it publicly (for example, 2 to 3 weeks).
- We disclose and broadcast the safety notice and correction on **our public channels**.

B. Rules

We ask you to respect the following rules at all times:

- Test vulnerabilities exclusively on your own deployments, on demo.oxygis.eu, or on your own trial instances of Oxygis Cloud.
- Never attempt to access or modify data that does not belong to you.
- Never attempt to carry out denial of service attacks or compromise the reliability and integrity of services that do not belong to you.
- Do not use scanners or automated tools to find vulnerabilities, as their effects could violate the above rules (unless you can guarantee that they will be limited to less than 5 requests/second and that they will not violate any other rules).
- Never attempt non-technical attacks, such as social engineering, phishing or physical attacks, against anyone or any system.
- Do not publicly disclose vulnerabilities without our prior consent (see also disclosure procedure above). During the non-disclosure period, you are permitted to use/test any fix we have provided, provided you do not emphasise the fix and do not publish it as a security report (i.e. you can use it on production servers).

C. In return :

- In the case of a test that complies with the rules set out above and does not cause any real harm, Oxygis undertakes not to initiate any civil or criminal proceedings against the reporter. We will process your report and respond to you as soon as possible.
- We will provide a fix as soon as possible

- We will work diligently with stakeholders and Customers to help them restore the security of their systems.
- We will not publicly disclose your identity if you do not wish to be credited for your discovery.
- This policy does not constitute a bug bounty programme. No payment will be made for reports.

III. What to report

Qualifying vulnerabilities - REPORT!

- SQL injection vectors in public API methods
- XSS vulnerabilities work in supported browsers
- Faulty authentication or session management, allowing unauthorised access.

Non-qualifying vulnerabilities - DO NOT REPORT!

- XSS vulnerabilities only work in unsupported or deprecated browsers, or require less stringent security settings.
- Auto-XSS attacks requiring the user to actively copy/paste malicious code into their own browser window.
- XSS attacks" by administrators, for example by downloading files (SVG, HTML, JS, etc.) or injecting scripts. Administrators are webmasters, the security restrictions do not apply to them, this is a feature.
- Speed limitation / brute force / scripting of components working as expected (e.g. password authentication, password reset, etc.).
- User registration (possibility of checking that a user name exists). Not very risky and cannot be avoided without damaging the user experience.
- Disclosures of file paths, which do not entail any significant risk and do not enable attacks that would otherwise be impossible.
- Clickjacking" or "phishing" attacks, which use social engineering tricks to trick users into making the system work as intended.
- Tabnapping or other phishing attacks carried out while browsing in other browser tabs
- CSRF disconnection (no plausible attack + cannot be prevented, e.g. by throwing cookies or overflowing the cookie box)
- Reflexive file downloads, another attack technique that requires social engineering and is not very practical.
- Leakage of referrers (including sensitive tokens) via social media links or advertising/analysis requests - very unlikely to be clicked, or exploited during the validity period by these mainstream companies!
- More generally, attacks based on physical or social engineering techniques will generally be rejected.
- Non-permanent Denial of Service (DoS) and Distributed DoS (DDoS) that keep resources (cpu/network/memory) exhausted via a sustained flow of requests/packets.

- Password policies (length, format, character classes, etc.)
- Missing or partial verification of e-mail addresses
- Disclosure of public information or information that does not involve any significant risk (the list of directories on our download archive is a mandatory feature! ;-))
- Anti-spam policies and systems, such as DKIM, SPF or DMARC.
- Absence of HTTP Strict Transport Security (HSTS) headers, HSTS preloading and HSTS policies.
- Attack scenarios including taking control of users' email accounts

If you have any doubts, ask us first!

Oxygis reserves the right to coordinate the public disclosure of a vulnerability in collaboration with the researchers involved and the parties concerned (clients, partners, competent authorities), in order to guarantee prior correction. Premature public disclosure without consultation could compromise this approach and could be excluded from the scope of protection defined in this policy.