Responsible Disclosure Policy

At Operator of the System, we consider the security of our systems - and our users - a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present. If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible.

Scope

The following areas are considered **out of scope**:

- Spam (unless a specific vulnerability leads to easily sending spam with implementation of System's data base);
- Security of applications or services, provided by third parties, which are external and not controlled by the System Operator;
- Integrations and extensions created by third party developers using our public API;
- Non-production environments across our product line;
- Distributed Denial of Service attacks (DDoS)
- Vulnerabilities in our open source software (unless you have a proof of concept of how the specific vulnerability can be used on Operator of the System .com or related apps);
- Missing security headers or 'best practices' (except if you are able to demonstrate a vulnerability that makes use of their absence);
- Social engineering attacks;
- Faults of hosting services at side of the User of our Services (on this issue, please contact your provider);
- Controversies in policies (verification, etc.).

The following areas are considered **in scope**:

- The Operator of the System on-line application;
- Website;
- System's mobile application;
- API;
- Data base.

What we ask of you

If you believe you have discovered a security vulnerability in System, please do the following:

- Submit your findings by using our e-mail address;
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data. This is critically important, so let us emphasise: *do not interact with the data in question more than is necessary to notify us.*
- Do not reveal the problem to others until it has been resolved.
- Do not use attacks on physical security, social engineering, distributed denial of service (or any attack using large volumes of requests), spam or applications of third parties.
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

What we promise

- We thank you for your help in making Operator of the System more secure;
- We will respond to your report accepted by e-mail with our evaluation of the report;
- If you have followed the instructions above, we will not take any legal action against you in regard to the report or pass on your personal details to third parties without your permission.
- We will keep you informed of the progress towards resolving the problem.
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise).

Recognition and remuneration

For accepted reports we may provide a financial reward. This reward will be based on the quality of the disclosure and nature of the vulnerability. Where possible we may also provide a Pro account (with a value of 120 EUR) and if available some Operator of the System swag.

Please feel free to submit your report anonymously or under a pseudonym. Rewards are granted entirely at our discretion, and may be reduced or declined if there is evidence of abuse.

Questions

If you have any questions regarding this Responsible Disclosure Policy, get in touch by sending an e-mail to: support@gioconostro.com.

Link to full text of Rules and Terms of Service