Responsible Disclosure Policy

Last edited: 01 November 2021

Created: 14 May 2020

Responsible disclosure policy
At expoze.io, 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.

Submit your findings by sending an e-mail to security@expoze.io.

Scope
The following areas are considered out of scope:

- Vulnerabilities that require access to an already compromised account (unless access to an account exposes other accounts)
- Policies as opposed to implementations - email verification, password length or reuse, etc.
- Ability to upload or download malicious files via the expoze.io platform
- Users hosting malware on our service (contact support for this)
- Spam (unless a specific vulnerability leads to easily sending spam)
- Authentication (or lack thereof) on free demo processing
- Missing security headers or 'best practices' (except if you are able to demonstrate a vulnerability that makes use of their absence)
- Vulnerabilities in our open source software (unless you have a proof of concept of how the specific vulnerability can be used on the expoze.io platform or related apps).
- Distributed Denial of Service attacks (DDoS)
- Social engineering attacks
- Third party applications we make use of, but do not control. (e.g. a blog hosted on an external service - unless we've configured the blog in such a way as to make our in-scope areas vulnerable)
- Integrations and extensions created by third party developers using our public API
- Non-production environments across our product line

The following areas are considered in scope:

- The expoze.io web application
- Other applications listed on our website
- Our API

Ideally, a reported vulnerability will be achievable without physical access to a target's device.

In addition, while we welcome disclosure reports from automated tools / scans, we cannot offer a reward.

What we ask of you
If you believe you have discovered a security vulnerability in an expoze.io service, please do the following:

- Submit your findings by sending an e-mail to security@expoze.io.
- 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 emphasize: 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 expoze.io more secure.
- 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 free account for a full year.

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 security@expoze.io.