Rocket Minds

Vulnerability Disclosure Policy

How do you report?

Send an email to us at info@rminds.nl with the following information:

- A summary of the vulnerability containing such info as URL and type of vulnerability.
- The necessary information that we need in order to reproduce the vulnerability that you have discovered.
- If applicable, a screenshot of the vulnerability you have found.
- Contact information, name, email, phone number etc.

Disclosure Policy

- Let us know as soon as possible upon discovery of a potential security issue, and we'll make every effort to quickly resolve the issue.
- Provide us a reasonable amount of time to resolve the issue and consult with us before any disclosure to the public or a third-party.

What will disqualify researchers from the program?

Researchers will not be eligible to participate in the program if they: make threats; demand money/payments/entry into program in exchange for bugs; publicly disclose without disclosure to Rocket Minds first; spam the security alias; degrade, interrupt or deny service to our users; modify, copy, download, delete or otherwise misuse other members’ data; access non-public member information without authorization; otherwise violate the Rocket Minds terms of use.

What can you expect from us?

We will respond to your report within 3 business days.
We will continue keep you informed of the progress towards resolving the problem.
We will treat your report confidentially and will never share your personal data with any third parties, except when we are legally forced to do so.

Qualifying Vulnerabilities

Any design or implementation issue that is reproducible and substantially affects the security of Rocket Minds's projects is likely to be in scope for the program. Common examples include:

Cross Site Request Forgery (CSRF).
Remote Code Execution (RCE).
Unauthorized Access to Properties or Accounts.

Non-Qualifying Vulnerabilities

Depending on their impact, not all reported issues may qualify for a monetary reward. However all reports are reviewed on a case-by-case basis and any report that results in a change being made will at a minimum receive recognition.

Please refrain from accessing private information, performing actions that may negatively affect Rocket Minds users (spam, denial of service), or sending reports from automated tools without verifying them.

The following issues are outside the scope of our vulnerability rewards program:

Attacks requiring physical access to a user's device or network.
Forms missing CSRF tokens (we require evidence of actual CSRF vulnerability).
Login/Logout CSRF.
Missing security headers which do not lead directly to a vulnerability.
Use of a known-vulnerable library (without evidence of exploitability).
Reports from automated tools or scans.
Social engineering of Rocket Minds staff or contractors.
Denial of Service attacks.
Mass account and file creation.
Results acquired by large scale automated test tools.
Not enforcing certificate pinning.