Security and vulnerability

Responsible Vulnerability Disclosure:

This page is for independent security researchers who are willing to report or want to start looking for, vulnerabilities on the ResearchGate platform.

The information on this page is intended only for security researchers who are interested in reporting security vulnerabilities on ResearchGate. If you are a ResearchGate account holder and have questions, you can contact our Support team here.

If you believe that you have discovered a security vulnerability on the ResearchGate platform, we strongly encourage you to inform us and to not disclose the vulnerability publicly. We appreciate your assistance, and we review all reports and do our best to address the issues within the specified time frame.

If you follow our guidelines and properly report a security vulnerability, ResearchGate will not file any kind of lawsuit nor ask law enforcement to investigate. In fact, helpful security disclosures can lead to rewards.

Responsible disclosure policy:

- You inform us immediately about any issue found.
- You make a good faith effort to avoid privacy violations and disruptions to others, including the destruction of data and the interruption or degradation of our services.
- You do not exploit a security issue you discover for any reason. This includes demonstrating additional risk, such as attempting to compromise sensitive company data or probing for additional issues.
- You do not make any information about your findings public, and you do not share such information with others.
- You refrain from creating a high volume of artificial content on digital property belonging to other users. You also make a sincere effort to create and use your own content for security tests.

The following vulnerability categories are considered out of the scope of our responsible disclosure program, and are not eligible for a bounty:

- Denial of Service (DoS)
- User / email enumeration
- Brute forcing
- Spamming which can be prevented by rate limiting techniques
- Vulnerabilities that involve a high amount of user interactions, such as social engineering
- Logout CSRF
- Outdated web browsers: vulnerabilities contingent upon outdated or unpatched browsers will not be honored
- Redirection from HTTP to HTTPS
- UI/UX bugs or spelling mistakes

Reporting a potential security vulnerability:

- Privately send details of the vulnerability to ResearchGate by sending an email to security@researchgate.net
- Provide full details of the vulnerability, including detailed steps on how to replicate it, so that we can validate the potential flaw.
- If you do not want to be publicly thanked on our hall of fame page (or elsewhere), please let us know in your report email that you want your submission to be confidential. We can still provide rewards for confidential submissions if requested.

Rewards:

- Not all reported issues may qualify for a reward. Rewards are awarded at ResearchGate's sole discretion.
- Only the first report we receive about a given vulnerability will be rewarded.
- Submissions that include detailed information on how to fix the corresponding vulnerability are more likely to receive more valuable rewards.
- Please note that we determine bounty amounts based on a variety of factors, including (but not limited to) impact, ease of exploitation, and the quality of the report. Note that extremely low-risk issues may not qualify for a bounty at all.

Changes to Terms and Conditions:

- The ResearchGate responsible vulnerability disclosure program, including its policies, is subject to change or cancellation by ResearchGate at any time, without notice. As such, ResearchGate may amend the terms and/or its policies at any time by posting a revised version on our website. By continuing to participate in the responsible vulnerability disclosure program after ResearchGate posts any such changes, you accept the terms, as modified.
Please note that the first assessment of a report can take up to 7 working days. Please refrain from asking for updates as we will only be able to respond once our security team has validated the vulnerabilities that you report.