Security and vulnerability

Responsible vulnerability disclosure

This page is aimed at independent security researchers who would like to report or look for vulnerabilities on our website researchgate.net, including any of its subdomains.

Please note that this information is intended for security researchers only – if you are a ResearchGate member and have questions, please **contact us**. Ou r Community Support team will get back to you.

Reporting potential security vulnerabilities

Firstly, we would like to thank you for your assistance. ResearchGate recognizes the contributions of security researchers who invest their time and effort to help make ResearchGate more secure.

The rewards we offer are based on the severity of the risk, however, we also consider the time taken to uncover it. If you believe that you've discovered a security vulnerability on the site, we strongly encourage you to inform us of this and not disclose the vulnerability publicly. We review all reports we receive and do our best to address issues reported to us within the specified timeframe.

Please take a moment to first read our Responsible Disclosure Policy and take note of the categories that fall outside of the scope of our responsible disclosure program.

Responsible Disclosure Policy

- You will inform us immediately about any issue found.
- You will 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 will 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 will 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.
- You will not interact with an individual account (which includes modifying or accessing data from the account) if the account owner has not consented to such actions.
- When experimenting, please only attack test accounts you control. A PoC that unnecessarily involves the accounts of other end users or ResearchGate employees may be disqualified.
- You will not run automated scans without checking with us first.
- You will not test the physical security of ResearchGate offices, employees, equipment, etc.
- You will not use social engineering techniques (phishing, etc.).
- You will not perform DoS or DDoS attacks even if you want to test for other vulnerabilities such as race conditioning.

The following vulnerability categories are outside of the scope of our responsible disclosure program, and aren't eligible for bounty:

- Denial of Service (DoS), or its distributed version (DDoS)
- User / email enumeration
- Brute forcing
- Spamming that can be prevented by rate limiting techniques
- Vulnerabilities that involve a high number of user interactions, such as social engineering
- CSRF on forms publicly available
- Missing SPF / DKIM / DMARC entries
- Redirection from HTTP to HTTPS
- UI / UX bugs or grammar/spelling mistakes
- Outdated web browsers – vulnerabilities contingent on outdated or unmatched browsers will not be compensated

How to report a vulnerability

Please send details of the vulnerability to ResearchGate via email to **security@researchgate.net.** Make sure that you provide the full details of the vulnerability, including detailed steps on how to replicate it, so that we can validate the potential flaw. If you don't want to be publicly thanked on our hall of fame page (or elsewhere), please let us know that you want your submission to be confidential – we can still provide rewards for confidential submissions if requested. Please note that ResearchGate reserves the right to publish and edit reports.

Please note: The first assessment of a report can take up to **7 working days**. Please don't contact us asking for an update as we will only be able to respond once our security team has validated the vulnerabilities you report.

Evaluation criteria and rewards

- We do our best to evaluate and respond to all acceptable reports we receive.
- We reward bugs after we fix them and if we need to fix them.
- We prioritize bugs based on risk and other factors, so it may take some time before you receive a reply.
- Not all reported issues will qualify for a reward – rewards are given 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.

- 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.
- We usually calculate risk and try to determine how critical it is using CVSS v3.
- We try to reward similar issues with similar compensation, but also consider the time taken to uncover it. Please note that we do not guarantee similar results or compensation for future reports.
- If you provide attack vectors it may affect the criticality of the vulnerability and could affect compensation.

Changes to the Terms and Conditions

The ResearchGate responsible vulnerability disclosure program, including all its policies, is subject to change or cancellation by ResearchGate at any time and 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: Provided that you follow our guidelines on how to report security vulnerabilities and our Responsible Disclosure Policy, ResearchGate will not file any kind of lawsuit or ask law enforcement to investigate.

Did you find the information you were looking for?

Get technical help **OR** Give us feedback **OR** Report a bug