neogames®

Responsible Disclosure Policy

neogames

1. Introduction

NeoGames welcomes feedback from security researchers and the general public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you. This policy outlines steps for reporting vulnerabilities to us, what we expect, what you can expect from us.

NeoGames ("We", "Us", "Our") appreciates and values the identification and reporting of security vulnerabilities carried out by well-intentioned, ethical security researchers ("You").

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us. We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

If you believe you have found a security vulnerability in our products, please tell us about it.

2. Systems in scope

This policy applies to any digital assets owned, operated, or maintained by NeoGames Ltd.

3. Out of scope

Assets or other equipment not owned by parties participating in this policy.

Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or applicable authority.

4. Our commitments

When working with us, according to this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed;
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints;

5. Our expectations

In participating in our vulnerability disclosure program in good faith, we ask that you:

- "Play by the rules", including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail;
- Report any vulnerability you've discovered promptly;
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience;
- Use only the Official Channels to discuss vulnerability information with us;

- Provide us a reasonable amount of time (at least 90 days from the initial report) to resolve the issue before you disclose it publicly;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), credit card data, or proprietary information;
- Do not engage in extortion.

6. How to report a security vulnerability to us

If you believe you have found a security vulnerability in one of our websites or products, we encourage you to let us know right away, providing all relevant information. The more details you provide, the easier it will be for us to triage and fix the issue.

We welcome reports from everyone, including developers, researchers and customers.

To report a security vulnerability, please contact us mailto:security@neogames.com and include the following information:

- The website domain, URL, IP address or webpage, where you found the issue. When did you find it.
- A description of the issue, including what you saw and what you expected to see.
- A list of steps to reproduce the issue (it should be a benign, non-destructive, proof of concept), or a video demonstration if it's a complicated issue. This helps to ensure that the report can be triaged quickly and accurately.

7. What to expect from us, and NeoGames handles vulnerability disclosure

We aim to confirm receipt of your vulnerability report within 5 working days and triage your report within 10 working days. We also aim to keep you informed of our progress and completion of any remediation activities. We may contact you if we require further information regarding your report.

Remediation of any reported vulnerabilities are assessed based upon their impact, severity, and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status, but we ask that you avoid doing so more than once every 14 days to allow our teams to focus on the remediation.

Please note that we do not offer a bug bounty program. This means that NeoGames does not pay rewards for disclosed security vulnerabilities.

To protect our customers, we investigate all reported issues, but we do not confirm them publicly.

8. What we kindly ask of you

You MUST NOT

- Break any applicable law or regulations.
- Access unnecessary, excessive, or significant amounts of data or modify data in our systems or services.
- Disrupt our services or systems, use high-intensity invasive or destructive scanning tools to find vulnerabilities or attempt any form of denial of service.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice", for example missing security headers.
- Submit reports detailing TLS configuration weaknesses, for example, "weak" cipher suite support or the presence of TLS1.1 support.
- Social engineer, 'phish' or physically attack our staff or infrastructure.
- Demand financial compensation to disclose any vulnerabilities.

You MUST

- Always comply with data protection rules and must not violate the privacy of our users, staff, contractors, services, or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

9. Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause us to be in breach of any legal obligations.