NOWPayments Bug Bounty Rules

Welcome to **NOWPayments'** bug bounty description! Please read all the rules before submitting your bug.

NB: Give us a reasonable amount of time before disclosing the vulnerability publicly – we need it to fix the bug and ensure our customers' safety!

Eligibility

In order to be eligible for the **Bug Bounty program**, kindly stick to the following requirements:

- Do not interrupt or harm our service intentionally.
- Do not defraud or harm **NOWPayments'** customers during your research.
- Do not use scanners or automated tools to find bugs.
- Do not attack the reliability or integrity of our services (e.g, no DDoS attacks or similar questionable acts).

If in doubt, please email us at support@nowpayments.io and we will provide you with all the necessary information.

Bounty Scope

All tools and services provided by **NOWPayments** are eligible for our Bug Bounty, including services offered through **NOWPayments API**, **NOWPayments' widgets, buttons, and invoice links**.

What are the Qualifying Bugs?

Any issues that could result in **substantial financial loss, customers' or internal data breach** qualify for the reward.

Which Bugs Don't Qualify for the Reward?

Depending on their impact, some disclosures may not qualify. Vulnerabilities in the **software packages not produced by NOWPayments, domains hosted by third parties, services operated by third parties based on NOWPayments APIs, and subdomains** are out of the Bug Bounty scope.

How to Disclose?

You can disclose a vulnerability by sending an email with your bug report to **support@nowpayments.io.**
Please include a **description of the bug and replication instructions** in your bug report.

Bounty Size and Payout

The bounty will be paid out **once the underlying issue has been resolved by our development team**. **Only the first person to report a certain bug will be rewarded.**

Reward size is determined individually and depends on the security impact in question. **NOWPayments** reserves the right to requalify the security impact. **All bounties are paid out in ETH or BTC (NOW token in some cases).**

Depending on the severity of the bug, the review process may take up to **20 business days.**

Bug severity

Critical ($500 +)

- Vulnerabilities exposing the user's confidentiality
- Vulnerabilities with adverse effect on stable operation of the platform and services
- Vulnerabilities leading to money loss

Examples:

- Database editing
- Merchant wallet reassignment via API request

High ($200 – $500)

- Vulnerabilities exposing the user's account to 3rd party manipulation
- Vulnerabilities affecting stable operation of the platform and services

Examples:

- Deletion of a different merchant's API key
- 2-factor authentication bypass

Medium ($50 – $200)

- Vulnerabilities affecting User Experience or causing minor disruptions to the flow.

Examples:

- Clickjacking issues
- User data leak

Low ($10 – $50)

- Vulnerabilities causing minor inconvenience to users or to the website's image

Examples:

- API error for correct request
- Frontend issues