Staking & RPC Infrastructure Bug Bounty Programme

Version 1.0 | 24 May 2026

01 Purpose and Scope

Node101 is committed to safeguarding the availability, integrity and confidentiality of its staking and RPC infrastructure. This programme invites independent security researchers to help identify potential weaknesses responsibly, so that issues can be assessed, remediated and disclosed in a coordinated manner.

02 In-Scope Research Areas

The programme is focused on security issues that could materially affect Node101-operated staking and RPC services, externally accessible infrastructure, or the protection of users and operational systems.

- Publicly accessible staking and RPC interfaces, dashboards and account or authentication flows operated by Node101.
- APIs, integrations and externally exposed infrastructure that support Node101 staking and RPC services.
- Authorization, session management, data exposure, workflow integrity and other vulnerabilities with a demonstrable security impact.

03 Rules of Engagement

Researchers must act in good faith and take reasonable steps to avoid harm. Testing should be limited to the minimum activity necessary to demonstrate a finding. Do not disrupt services, access or retain personal or confidential data, alter user accounts or assets, conduct social engineering, or perform denial-of-service testing.

NODE101 TEKNOLOJİ A.Ş. (Inc.)
Karanfil Sokak, Villa 13 Levent, Beşiktaş, Istanbul,
Republic of Turkiye, 34330
hello@node101.io

Reporting and response

A coordinated process for high-quality vulnerability reports.

04 Vulnerability Reporting Procedure

Submit reports through the dedicated security reporting channel published in the Node101 Trust Center. A high-quality report should include a clear description of the issue, affected asset or service, reproducible steps, the observed impact, and any proof of concept that is safe to share. Please provide only the evidence necessary to validate the finding.

05 Vulnerability Management Process

Node101 reviews received reports for scope, validity and potential impact. Where additional information is needed, we may contact the reporter through the submitted channel. Valid findings are prioritised according to risk and handled through our security and engineering processes. We ask researchers to keep report details confidential while remediation is in progress.

- Receipt and initial assessment of the report.
- Technical validation and impact review.
- Remediation, verification and coordinated communication when appropriate.

06 Prohibited Activities

The programme does not authorise testing of third-party systems, networks, wallets, exchanges, cloud providers or protocols that are not operated by Node101. It also excludes physical attacks, phishing, social engineering, spam, service disruption, destructive testing, and any activity that may endanger users, funds, data or service availability.

07 Programme Terms and Governance

This announcement forms part of Node101's broader commitment to security, operational resilience and transparent infrastructure practices. Programme scope, eligibility and handling procedures may be updated as services evolve. Participation is subject to applicable law and to the terms published in the Node101 Trust Center.