RSK Vulnerability Bounty Program

RSK Labs Ltd (“RSK”) has created a vulnerability bounty program to reward security researchers that dedicate time and effort to improve the RSK platform. If you think you’ve found a vulnerability in RSK public blockchain, please send your report to:

security@rsk.co

If you consider the finding to be of high or critical security, please submit your report encrypted to the PGP public key that can be downloaded from here:

https://bountyprogram.rsk.co/

The PGP key fingeprint is: 69F6 F997 2497 8762 D541 8AE4 58D2 260D 5998 6758

The report should be written in English, and it shall include:

- Short description
- Attack scenario
- Software components & affected versions
- Instructions to reproduce
- Details
- if necessary: test code, scripts, data sets.

Your contribution will be rewarded according to the Rules specified in the current program. Many areas of vulnerability research are shared with the Ethereum bug bounty program to facilitate co-reporting.

Vulnerabilities that also Apply to Other Compatible Platforms

If you find a vulnerability that applies simultaneously to RSK, Ethereum, Ethereum Classic or any other EVM/Web3-compatible platform, you should decide which platform security teams you will trust, and privately report the vulnerability to those security teams. We suggest you do it simultaneously in a single email. We will do our best effort to coordinate fixing and public disclosure with the other teams that you choose to report to, to prevent collateral damage. If we think other security teams should be involved, we may forward the information to those teams. RSK won’t collect third party bug bounties.

We’ll try to keep people’s digital assets safe in every platform that we think may be affected. However, we cannot assure a coordinated response with other security teams, as each team may have different rules, neither we have any influence in bounty programs from other platforms.

Rules

- The submitter must be the person who has discovered the vulnerability. Vulnerability submission cannot be delegated.
- We accept anonymous submissions, but in that case the bounty reward will be donated to charity.
- The submitter grants RSK the right to use parts or all the submitted report for communicating the vulnerability to the public.
- RSK may cite the submitter name and points earned in RSK blog posts and online bounty rankings.
- if you prefer not to be identified in RSK communications by your real name you must clarify this and provide a pseudonym in your submission.
- Issues that have already been submitted by another user or are already known to the RSK team are not eligible for bounty rewards.
- Public disclosure of a vulnerability makes it ineligible for a bounty. If the user reports the vulnerability to other security teams (e.g. Ethereum or ETC) but reports to RSK with considerable delay, then RSK may reduce or cancel the bounty.
- You can start or fork a private chain for bug hunting. Please refrain from attacking the RSK mainchain and test networks. Also please refrain from attacking the ETH or ETC main-chains and test networks. An attack will make the vulnerability ineligible for a bounty.
- RSK development team, employees and all other people paid by RSK , directly or indirectly, are not eligible for rewards.
- A person who submitted a change in the RSK codebase is not eligible for rewards for vulnerabilities originating or triggered by the submitted change.
- RSK websites, infrastructure and assets are NOT part of the bounty program.
- RSK bounty program considers a number of variables in determining rewards. Determinations of eligibility, score and all terms related to an award are at the sole and absolute discretion of RSK.

The value of rewards paid out will vary depending on **severity**. The severity is calculated according to the OWASP risk rating model based on *Impact* and *Likelihood* :

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Examples:

- A bug triggered by a single low-cost transaction that forks the RSK blockchain into some nodes accepting a block containing the transaction and some nodes rejecting that block, will be generally considered High. This is because it is highly likely to be used for an attack but the impact is medium, because a double-spend attack must also be perpetrated to steal assets.
- A remote attack to a specific node that steals its private keys with some very low probability will be generally considered High. This is because the impact is high but the likelihood is medium, and many nodes must be probed until the attacker finds the right victim.
- An attack that spams the blockchain or the state with a cost much lower than the expected, will be generally considered Medium.
- A remote attack that reveals some private information of a node that does not lead to the loss of funds will be generally considered Low.

Reward sizes are *guided* by the rules below, but are in the end, determined at the sole and absolute discretion of RSK security team.

- **Critical**: up to 25 000 points
- **High**: up to 15 000 points

- **Medium**: up to 10 000 points
- **Low**: up to 2 000 points
- **Note**: up to 500 points

The USD/point rate will be increased as the platform matures. At launch, starting from December 4th, 1 point corresponds to 0.2 USD (payable in BTC, ETH or Bank Transfer, as of RSK convenience). We may change the USD/point rate without prior notice by updating the rate in our website. Beyond monetary rewards, every bounty is also eligible for listing on our leaderboard with points accumulating over the course of the program.

In addition to Severity, other variables are also considered by the RSK security team to modify the score, such as:

- **Quality of description**. Higher rewards are paid for clear, well-written submissions.
- **Quality of reproducibility**. The easier it is for us to reproduce and verify the vulnerability, the higher the reward. Please include test code, scripts and detailed instructions.
- **Quality of fix, if included**. Higher rewards are paid for submissions with clear description of how to fix the issue.

Important Legal Information

- The bug bounty program aims to encourage the academic, hacker, and development communities to analyze the RSK platform and help improving it.
- RSK can cancel the program at any time, at its sole criteria and decision. Also, RSK has the full and exclusive right and power to modify or amend, at its sole decision, the terms and conditions of the program, including the rewards rules. The changes will come into effect on the revision date shown in the revised terms. By continuing to use the program you are agreeing to the revised terms.
- Every award, reward and/or payment to be done under this terms and conditions of the program shall be determined at the sole discretion of RSK. All award, reward and/or payment are subject to applicable law.
- In addition, RSK is not able to issue awards to individuals who are on sanctions lists or who are in countries on sanctions lists set forth by the Organization for Economic Co-operation and Development (OECD).
- You will be the only and exclusive responsible for all the applicable taxes accrued over the rewards and/or payment to be done under this program.
- In order to receive the applicable reward, your vulnerability research must not violate any law or compromise any data that is not of your property. In addition, RSK will not be responsible for any breach or violation of any third party right or property that you may had incurred during your testing process and your participation in the program. To the fullest extent permitted by law, you shall defend, indemnify and hold harmless RSK and its respective members, partners, managers, officers, affiliates, employees, agents and

assignees from and against any and all liability (common law, equitable, statutory and/or punitive), claims, suits, losses, damages, demands and expenses (including, without limitation, reasonable attorneys' fees and costs) brought by third parties arising out of, or related to, your testing process or vulnerability research.

- In consideration of the vulnerability reports and the assignments mentioned hereof, RSK will pay you the reward which will be set forth at the sole discretion of RSK using the different rules mentioned hereby.
- To the maximum extent permitted by applicable law, you hereby release and waive all claims against RSK, its subsidiaries, affiliates, officers, agents, licensors, co-branders or other partners, and employees (Hereinafter, the "Representatives") from any and all liability for claims, damages (indirect, special, incidental, punitive, actual and/or consequential), costs and expenses (including litigation costs and attorney's' fees) of every kind and nature, arising from or in any way related to your participation in the Program. In addition, you expressly waive and relinquish any and all rights and benefits which you may have under any particular state or federal statute or law principle to the fullest extent permitted by law.
- Participants in the Program understand and acknowledge that through their participation there´s no creation, and should not be interpreted or construed as creating, any agency, partnership, joint venture, franchise, or employment relationship between the participant and RSK.
- If any provision of this Program is found to be invalid (partially or totally), participants nevertheless agree to give effect to RSK´s intentions as reflected in the provision and that the other provisions remain in full force and effect.
- This Terms & Conditions shall be governed by and construed in accordance with the laws of the British Virgin Islands. State of New York without regard to principles of conflicts of law.
- Any and all differences, controversies and disputes of any nature whatsoever arising out of or relating to this Program, including any dispute relating to its validity, interpretation, performance or termination, shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce by three arbitrators appointed in accordance with said Rules. The arbitration proceedings shall be conducted in the English language and the seat of the arbitration shall be the British Virgin Islands. The arbitrators appointed in connection herewith shall be knowledgeable in the laws of the British Virgin Islands and fluent in the English language. All submissions and awards in relation to arbitration under this Terms shall be made in English, and all arbitration proceedings and all pleadings shall be in English. Witnesses not fluent in English may give evidence in their native tongue (with appropriate translation). Original documents in a language other than English shall be submitted as evidence in English translation accompanied by the original or true copy thereof. The procedural rules governing arbitration hereunder shall be established by the arbitrators; provided that (i) each party may call upon the other party to supply the arbitrators with documents in such other party's control relevant to the dispute; (ii) each party shall be entitled to present the oral testimony of witnesses as to fact and expert witnesses; (iii) each party shall be entitled to question directly any witnesses who present testimony to the arbitrators and (iv) at the request of any party, a written transcript in English shall be made of each hearing before the arbitrators and shall be furnished to the parties. The arbitrators may, at the

request of any party, order provisional or conservatory measures; provided that to the extent necessary to prevent irreparable damage any party may petition any court of competent jurisdiction for a preliminary injunction, temporary restraining order or other interim equitable relief pending the appointment of the arbitrators and action by the arbitrators upon any request for provisional or conservatory measures. Each party participating in such arbitration shall pay its own legal fees and expenses incurred in connection with the arbitration and the expense of any witness produced by it. The cost of any stenographic record and all transcripts thereof shall be pro-rated equally among all parties ordering copies and shall be paid by the parties directly to the reporting agency. All other expenses of the arbitration, including required traveling and other expenses and fees of the arbitrators and the expenses of any witness or the cost of any proof produced at the request of the arbitrators, shall be borne as determined by the arbitrators. Any award shall be final and not subject to appeal and the parties waive all rights to challenge any award of the arbitrators. Any award may be entered or presented by any of the parties for enforcement in any court of competent jurisdiction sitting in the British Virgin Islands, and the parties hereby consent to the jurisdiction of such court solely for purposes of enforcement of any award.

Open Bounties

Our bug bounty program spans end-to-end: from soundness of protocols (such as the blockchain consensus model, the wire and p2p protocols, proof of work, etc) and protocol implementation. Classical client security as well as security of cryptographic primitives are also part of the program. Details on the scope follow:

Protocol Design security

RSK protocol stack has some similarities with Ethereum, but differs in many ways. Most of the protocols, such as consensus, blockchain synchronization, state trie and EVM have been redesigned or modified. As there is no currently formal description of these new protocols, vulnerabilities in the protocol design would be evaluated against the intended functionality, which may not be evident.

We encourage researchers to look for problems in the design of the following areas:

- Bitcoin Bridge (two way peg)
- Federation members management
- Block difficulty adjustment algorithm
- Selfish mining incentives
- SPV security
- Uncle mining incentives
- State Trie security
- Misaligned / unintended economic incentives and game theoretic flaws.
- Security weaknesses / attacks on the PoW algorithm or Merge-Mining system.

- A concrete example could be a contract that consumes very little gas but leads to a lot of computational effort effectively opening the door for DoS attacks.

Implementation security

Client protocol implementation security

Assuming that the protocols and algorithm designs are flawless, does a client implementation conform to the intended behaviour? Issues could include:

- Validations of blocks, transactions and messages
- RSK Virtual Machine code execution
- Transaction execution
- Contract creation
- Message calls
- Calculation and enforcement of gas and fees

Network security

This category focuses on generalized attacks on the whole network or a subset of it:

- 51% and other low x% attacks.
- Isolation attacks
- Finney attacks.
- Sybil attacks.
- Replay attacks.
- Transaction / messages malleability.
- (global) DoS.

Node security

Attacks on a single RSK client relating to the RSK platform:

- DoS / resource abuse
- Account / wallet address gathering/probing
- Broadcast / withhold attacks

Application security

This category addresses more classical security issues:

- Data type overflow / wrap around, e.g. integer overflow.
- Panics or not properly handled errors.
- Concurrency, e.g. synchronization, state, races.
- Issues related to external libraries used.

Applied Cryptographic security

This category includes:

- Incorrect implementation / usage / configuration of:
- Elliptic curve (secp256k1, ECDSA).
- Hash algorithms (Keccak-256).
- Merkle Patricia trees.
- Key management
- Random source quality
- Side channels and information leaks