Tezos Foundation Comments on the Least Authority Vesting Smart Contracts Audit Report

DRAFT: 26 February 2019

Compiled/Maintained by Ryan Lackey (Tezos Foundation) <ryan.lackey@tezos.com>
Answers from Nomadic Labs and others

Overview

The Tezos Foundation engaged Least Authority to perform an independent third-party audit of the Tezos project codebase in 2018. We are pleased with both the process and the result, and are appreciative of the depth and quality of review performed. Based on the report provided to us, we have the following response and comments on the report and our remediation efforts.

This report/response addresses the smart contract security of vesting contracts.

Issues

Issue A : Rejection of valid data

This issue does exist, but since the fault is attributable and since it is possible to re-submit the request without the invalid signature, it is not a viable vector for denial of service. This issue would be more significant for contracts involving a larger number of potential signers.

Issue B: Possible to create invalid contracts

This is more interesting because it is valid for all smart contracts. The mitigation is more complex. It is a decision of tezos to build a Turing complete language for its smart contracts. This allows our users to create almost any contract they can imagine, at the cost of making it harder for us to prove properties before testing. Determining statically the properties of the program before running it is an open research problem, and we are constantly working in this domain through formal verification and static analysis to prove the desired properties.

Issue C: Incorrect error locations

There is a bug in that the actual michelson parser does not track macro locations correctly. It is currently being rewritten by a developer who is aware of this issue and will fix it.

Suggestions:

Suggestion 1: Documentation inconsistencies

We are aware of several of these and are improving documentation.

Other Observations:

Insecure RPC between tezos-client and tezos-node

We have mitigated this issue to some extent by the documentation change identified, recommending that communications be restricted to localhost. We are waiting on cohttp to support TLS authentication, but are investigating other RPC mutual authentication.

Insecure installation process

This is an area of active improvement. We already started signing our commits, on release, we have the intention to sign tags and downloadable archives, and we will improve our handling of external dependencies. The opam repository has been pinned with sha256. Additionally, we are investigating other ecosystem-level ways to handle code signing, audit reporting, and interoperability.

Conclusion

We appreciated the opportunity to work with Least Authority on an independent security review of the Tezos software, and feel the process has resulted in identified issues which have been remediated, as well as better understanding of areas for future development effort and particular security concern within the system. We look forward to future security reviews by third parties as the system evolves.