Puffer Finance xERC20 and Validator Pricer

June, 2024

Made with ❤ by the following Creed authors: Valentin Quelquejay, Dominik Muhs

Table of Contents

Executive Summary

This report presents the results of our engagement with Puffer Finance to review their latest round of changes, including the new xERC20 implementation, as well as the validator ticket pricer and the updated timelock smart contracts.

The review was conducted over one week, from June 3rd, 2024 to June 7, 2024, by Valentin Quelquejay and Dominik Muhs. A total of ten person-days were spent.

No critical/high security issues were identified during the review. The set of changes in scope is simple and well-written, and the xERC20 implementation is very close to the reference implementation, which has been scrutinized by Creed in the past.

Scope and Objectives

Our review focused on the following commit hashes:

- PufferPool: `af17eaf29b09246ab2a4e88260def2cfe7591228`
- PufETH: `10580523278776018b7f51d6a704ba2dd3c580fe`

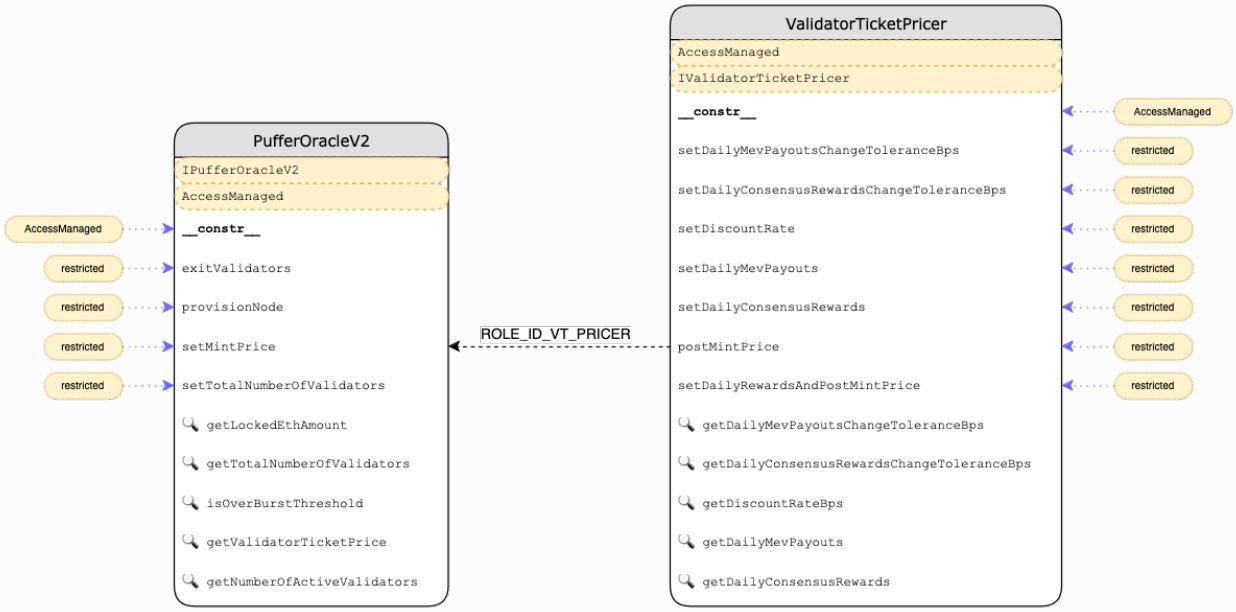
Specifically, the scope focused on the following pull request changes: PufferPool #260, pufETH #80, and pufETH #82.

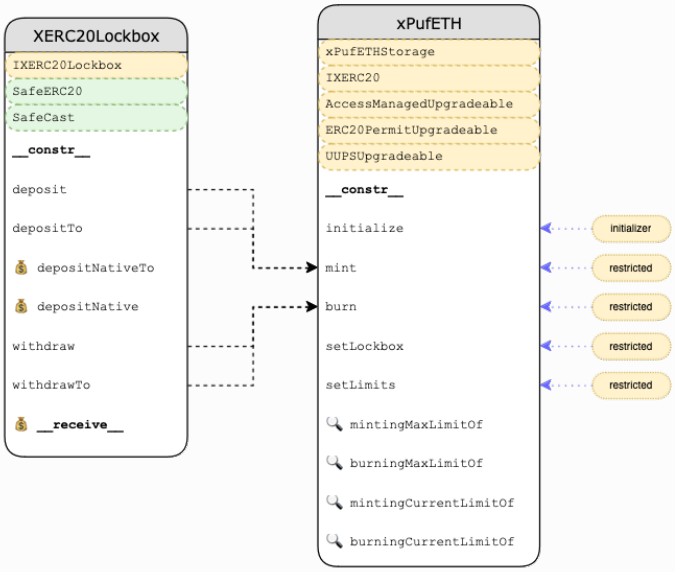
As part of the mitigation review, Creed reviewed puffer-contracts #3.

Together with the Puffer Finance team, we identified the following priorities for our review:

- Review potential cross-chain security issues in the xERC20 implementation.
- Ensure that the system is implemented consistently with the intended functionality, and without unintended edge cases.
- Identify known vulnerabilities particular to smart contract systems, as outlined in our Smart Contract Security Field Guide, and the ones outlined in the EEA EthTrust Security Levels Specification.

Audit Artifacts





Findings

Minor Incorrect Roles during Deployment

Acknowledged

The `Timelock` contract expects a variety of actors in its constructor. During the deployment process in `DeployL2XPufETH.s.sol`, all the relevant actors (operations, pauser, community) are set to the same broadcaster address.

pufETH/script/DeployL2XPufETH.s.sol

```
44 operationsMultisig = _broadcaster;
45 pauserMultisig = _broadcaster;
46 communityMultisig = _broadcaster;
```

Recommendation

We recommend verifying and using the environment variables' values to set each role's address.

None Inconsistencies in the input validation of private/public `setPauser` and `setDelay` functions

Fixed

This issue has been addressed in commit [b0b27934882327ac29e948b492441e4409c03fce](b0b27934882327ac29e948b492441e4409c03fce).

The `setPauser` and `setDelay` functions are designed to update critical parameters but have inconsistencies in where validation checks are performed:

- setPauser: Validates the new pauser address within the public function before calling the internal function.
- setDelay: Performs delay validation inside the internal `_setDelay` function and not the public function.

pufETH/src/Timelock.sol

```
281 if (newPauser == address(0)) {
282     revert BadAddress();
283 }
```

pufETH/src/Timelock.sol

```
293 if (newDelay <= MINIMUM_DELAY) {
294     revert InvalidDelay(newDelay);
295 }
```

We recommend performing the validation checks by moving the zero address validation from the public `setPauser` function to the private `_setPauser` function, ensuring all checks are performed within the private functions for consistency.

File Hashes

- ./code/PufferPool/src/ValidatorTicketPricer.sol
  - 4fb7d2fccaf394e835d69ce82e3ddab16ed9b6734c4ee61b8b3906f58600ba9b
- ./code/pufETH/src/l2/xPufETHStorage.sol
  - 874df01cbc6064a2d1ef33289f97dca4716a128eea738c285052de5339faf480
- ./code/pufETH/src/l2/xPufETH.sol
  - 40747702d47b34a958d78c121a88a9644195edf97db66454402f1fe4ffc68f00
- ./code/pufETH/src/Timelock.sol
  - d8a733b32049ba12bb9bbe31fb7bfc51e54393bf8fd9a494e9d30a7a846304ac
- ./code/pufETH/src/XERC20Lockbox.sol
  - a8c7d825501ea1fcf856e4af0e2ceb8122200a9933cf50ce42b592e2b191ef64

Disclaimer

Creed (“CD”) typically receives compensation from one or more clients (the “Clients”) for performing the analysis contained in these reports (the “Reports”). The Reports may be distributed through other means, including via Creed publications and other distributions.

The Reports are not an endorsement or indictment of any particular project or team, and the Reports do not guarantee the security of any particular project. This Report does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. No Report provides any warranty or representation to any Third-Party in any respect, including regarding the bugfree nature of code, the business model or proprietors of any such business model, and the legal compliance of any such business. No third party should rely on the Reports in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. Specifically, for the avoidance of doubt, this Report does not constitute investment advice, is not intended to be relied upon as investment advice, is not an endorsement of this project or team, and it is not a guarantee as to the absolute security of the project. CD owes no duty to any Third-Party by virtue of publishing these Reports.

PURPOSE OF REPORTS The Reports and the analysis described therein are created solely for Clients and published with their consent. The scope of our review is limited to a review of code and only the code we note as being within the scope of our review within this report. Any Solidity code itself presents unique and unquantifiable risks as the Solidity language itself remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond specified code that could present security risks. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. In some instances, we may perform penetration testing or infrastructure assessments depending on the scope of the particular engagement.

CD makes the Reports available to parties other than the Clients (i.e., “third parties”) – on its website. CD hopes that by making these analyses publicly available, it can help the blockchain ecosystem develop technical best practices in this rapidly evolving area of innovation.

LINKS TO OTHER WEB SITES FROM THIS WEB SITE You may, through hypertext or other computer links, gain access to web sites operated by persons other than CD. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites' owners. You agree that CD are not responsible for the content or operation of such Web sites, and that CD shall have no liability to you or any other person or entity for the use of third party Web sites. Except as described below, a hyperlink from this web Site to another web site does not imply or mean that CD endorses the content on that Web site or the operator or operations of that site. You are solely

responsible for determining the extent to which you may use any content at any other web sites to which you link from the Reports. CD assumes no responsibility for the use of third party software on the Web Site and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

TIMELINESS OF CONTENT The content contained in the Reports is current as of the date appearing on the Report and is subject to change without notice. Unless indicated otherwise, by CD.