Zellic

Beefy Token

Smart Contract Review

August 30, 2023

Prepared for:

Kexley

Beefy Finance

Prepared by:

Mohit Sharma

Zellic Inc.

About Zellic

Zellic was founded in 2020 by a team of blockchain specialists with more than a decade of combined industry experience. We are leading experts in smart contracts and Web3 development, cryptography, web security, and reverse engineering. Before Zellic, we founded perfect blue, the top competitive hacking team in the world. Since then, our team has won countless cybersecurity contests and blockchain security events.

Zellic aims to treat clients on a case-by-case basis and to consider their individual, unique concerns and business needs. Our goal is to see the long-term success of our partners rather than to simply provide a list of present security issues. Similarly, we strive to adapt to our partners' timelines and to be as available as possible. To keep up with our latest endeavors and research, check out our website zellic.io or follow @zellic_io on Twitter. If you are interested in partnering with Zellic, please email us at hello@zellic.io or contact us on Telegram at https://t.me/zellic_io.

1   Introduction

We were asked to review a small contract which is used to initialize an ERC20 token (BIFI) and mint an initial amount of eighty thousand tokens.

1.1   Scope

The engagement involved a review of the following targets:

Beefy Token

Repository	https://etherscan.io/address/0xb1f1ee126e9c96231cc3d3fad7c08b4cf873b1f1
Type	Solidity
Platform	EVM-compatible

Contact Information

The following consultants were engaged to conduct the assessment:

Mohit Sharma, Engineer
mohit@zellic.io

1.2   Disclaimer

This assessment does not provide any warranties about finding all possible issues within its scope; in other words, the evaluation results do not guarantee the absence of any subsequent issues. Zellic, of course, also cannot make guarantees about any additional code added to the assessed project after the audit version of our assessment. Furthermore, because a single assessment can never be considered comprehensive, we always recommend multiple independent assessments paired with a bug bounty program.

For each finding, Zellic provides a recommended solution. All code in these recommendations are intended to convey how an issue may be resolved (i.e., the idea), but they may not be tested or functional code.

Finally, the contents of this assessment report are for informational purposes only; do not construe any information in this report as legal, tax, investment, or financial advice. Nothing contained in this report constitutes a solicitation or endorsement of a project by Zellic.

2 Smart Contract Review

2.1 Contract overview

The `initialize` function in BIFI.sol accepts an address for a treasury contract, initializes an ERC20 token named "Beefy" with the symbol "BIFI", and mints an initial amount of eighty thousand tokens to the provided treasury address.

During our assessment, we did not identify any significant problems in the implementation.

One minor recommendation would be to include a check that ensures the provided treasury address is not a 0 address, as minting tokens to a 0 address could lead to token loss.