Blerb Finance Security Audit

Report Version 1.0

June 4, 2024

Conducted by **Hunter Security**:

Stormy, Senior Security Auditor
George Hunter, Peer Reviewer

Table of Contents

1 About Hunter Security

Hunter Security consists of multiple teams of leading smart contract security researchers. Having conducted over 100 security reviews and reported tens of live smart contract security vulnerabilities protecting over $1B of TVL, our team always strives to deliver top-quality security services to DeFi protocols. For security audit inquiries, you can reach out to us on Telegram or Twitter at *@georgehntr*.

2 Disclaimer

Audits are a time-, resource-, and expertise-bound effort where trained experts evaluate smart contracts using a combination of automated and manual techniques to identify as many vulnerabilities as possible. Audits can reveal the presence of vulnerabilities **but cannot guarantee their absence**.

3 Risk classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	High	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

3.1 Impact

- **High** - leads to a significant loss of assets in the protocol or significantly harms a group of users.
- **Medium** - involves a small loss of funds or affects a core functionality of the protocol.
- **Low** - encompasses any unexpected behavior that is non-critical.

3.2 Likelihood

- **High** - a direct attack vector; the cost is relatively low compared to the potential loss of funds.
- **Medium** - only a conditionally incentivized attack vector, with a moderate likelihood.
- **Low** - involves too many or unlikely assumptions; offers little to no incentive.

3.3 Actions required by severity level

- **High** - client **must** fix the issue.
- **Medium** - client **should** fix the issue.
- **Low** - client **could** fix the issue.

4 Executive summary

Hunter Security was engaged by Blerb Finance to review their smart contract protocol during the period from May 28, 2024, to June 1, 2024.

Overview

Project Name	Blerb Finance
Repository	https://github.com/dragon-software-devs/hybrid-defi
Commit hash	cc88fa06c12bf9df0661e97b0ba14fe62135d0a5
Resolution	5326fb8086186635280885146ab31de8871677b7
Methods	Manual review & testing

Timeline

-	May 28, 2024	Audit kick-off
v0.1	June 1, 2024	Preliminary report
v1.0	June 4, 2024	Mitigation review

Scope

contracts/Airdrop.sol
contracts/Bridge.sol
contracts/NFT.sol
contracts/Referral.sol
contracts/Token.sol
contracts/lib/*

Issues Found

High risk	0
Medium risk	0
Low risk	1

5 Findings

5.1 Low

5.1.1 Incorrect calculation of the genesis share may not allow pulling of commissions until the mint phase is closed

Severity: Low

Context: Bridge.sol#L262-L281

Description: The function *mintAndForward* is used by users in order to mint an early launch phase NFTs, the current price of an NFT token is 0.1 ether and is allocated to the following purposes:

- 25% of the price goes for the referrer commissions.
- another 25% goes to the liquidity providers.
- and the rest 50% goes for genesis shares.

However, as seen in the snippet below, the system doesn't always add commission to the user's referral which can happen in a case of revert. In this case commission was not added and sent to the referral contract, but this isn't taken into account and the system still calculates the genesis share like before. As a result the actual genesis share available in the Bridge contract is more than the accounted one in storage, which leads to the owner not able to withdraw the full amount until the mint phase is closed.

```
// Payout commission
if (referral.canAddCommission(user, address(0))) {
    uint256 commission = (ethForMint *
        Constants.REFERRER_COMMISSION) / Constants.BASIS;

    try
        referral.addCommission{value: commission}(
            user,
            address(0),
            commission
        )
    {
        // noop
    } catch {}
}

// Account for genesis
_genesisShare +=
    (ethForMint * Constants.ETH_FOR_GENESIS) /
    Constants.BASIS;
```

Recommendation: Consider adding the referrer commission to the genesis share in the cases when the commission can not be added to the referrer.

Resolution: Resolved.