SB SECURITY

Titan Legends Warlords

Security Review

Oct 8, 2024

Conducted by:
Blckhv, Security Researcher
Slavcheww, Security Researcher

Contents

1. About SBSecurity

SBSecurity is a duo of skilled smart contract security researchers. Based on the audits conducted and numerous vulnerabilities reported, we strive to provide the absolute best security service and client satisfaction. While it's understood that 100% security and bug-free code cannot be guaranteed by anyone, we are committed to giving our utmost to provide the best possible outcome for you and your product.

Book a Security Review with us at sbsecurity.net or reach out on Twitter @Slavcheww.

2. Disclaimer

A smart contract security review can only show the presence of vulnerabilities **but not their absence**. Audits are a time, resource, and expertise-bound effort where skilled technicians evaluate the codebase and their dependencies using various techniques to find as many flaws as possible and suggest security-related improvements. We as a company stand behind our brand and the level of service that is provided but also recommend subsequent security reviews, on-chain monitoring, and high whitehat incentivization.

3. Risk classification

	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	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** - leads to a moderate loss of assets in the protocol or some disruption of the protocol’s functionality.
- **Low** - funds are not at risk.

3.2. Likelihood

- **High** - almost **certain** to happen, easy to perform, or highly incentivized.
- **Medium** - only **conditionally possible**, but still relatively likely.
- **Low** - requires specific state or **little-to-no incentive**.

3.3. Action required for severity levels

- High - **Must** fix (before deployment if not already deployed).
- Medium - **Should** fix.
- Low - **Could** fix.

4. Executive Summary

Warlords are a generative NFT collection which consists of 8,888 unique and burnable NFTs, each costing 88,888 $LGNDX to be minted. NFTs can be minted, reminted and claimed. Each operation has a 3% burn fee in form of $LGNDX which is burned automatically.

Overview

Project	Titan Legends - Warlords
Repository	Private
Commit Hash	e3a3601a0202e5f97974ce86aba7cb74b05f087f
Resolution	73fba2872b2148e9f213565003cf5a3dc4d20b53
Timeline	October 8, 2024

Scope

WarChest.sol

Issues Found

Critical Risk	0
High Risk	0
Medium Risk	3
Low/Info Risk	0

5. Findings

5.1. Medium severity

5.1.1. mint is used instead of safeMint

Severity: Medium Risk

Description: The usage of mint is disregarded because it does not check whether the recipient can manage ERC721 tokens. As a result, if a Warlord NFT is minted to such an account, there is a risk that the tokens will be permanently locked if the contract does not have the functionality to at least claim the tokens.

```
function mint(uint256 amount) external {
    if (!isSaleActive) revert SaleInactive();
    if (amount == 0) revert ZeroInput();
    if (_totalMinted() + amount > maxSupply) revert SupplyExceeded();
    uint256 burnSum = amount * burnFee; //
    uint256 totalSum = amount * price + burnSum;
    LegendX.safeTransferFrom(msg.sender, address(this), totalSum);
    LegendX.burn(burnSum);
    _mint(msg.sender, amount);
    emit Mint(amount);
}
```

Recommendation: Consider using the _safeMint function from ERC721A, without the need to add the nonReentrant modifier.

Resolution: Fixed

5.1.2. Router approval is not zeroed

Severity: Medium Risk

Description: Since `_swapTitanXForLGNDX` will only use the TitanX that is needed for the `amountOut` LGNDX, at first the router is approved with `amountInMaximum`, but if the full amount is not used, the reminder is returned to the user. In this case, the approval for the router is not reset and the balance that is refunded to the user is still an allowance.

Recommendation: When returning the leftover, reset the allowance for the Router.

Resolution: Fixed

5.1.3. twap check should be based on `amountOutput`

Severity: Medium Risk

Description: Since the swap done here is with `exactOutput` and the protocol has an exact number of LGNDX, no matter how much TitanX it will cost, the twap check should be with upper bound and adding 20%, not like `exactInput` where subtract 20%.

Recommendation: Use an upper limit and add 20% above the original deposited and if the price of twap is higher revert.

Resolution: Fixed