# Cyberscope

## Audit Report

# My Bro

December 2024

# Analysis

● Critical ● Medium ● Minor / Informative ● Pass

| Severity | Code | Description | Status |
|----------|------|-------------|--------|
| ● | ST | Stops Transactions | Passed |
| ● | OTUT | Transfers User's Tokens | Passed |
| ● | ELFM | Exceeds Fees Limit | Passed |
| ● | MT | Mints Tokens | Passed |
| ● | BT | Burns Tokens | Passed |
| ● | BC | Blacklists Addresses | Passed |

# Table of Contents

# Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

| Severity | Likelihood / Impact of Exploitation |
|---|---|
| ● Critical | Highly Likely / High Impact |
| ● Medium | Less Likely / High Impact or Highly Likely/ Lower Impact |
| ● Minor / Informative | Unlikely / Low to no Impact |

# Review

| Repository | https://github.com/breadNbutter42/BRO/tree/main |
| --- | --- |
| Commit | 073f35103199e533d0873da89805e18172fd01e9 |

## Audit Updates

| Initial Audit | 10 Dec 2024 |
| --- | --- |
| | https://github.com/cyberscope-io/audits/blob/main/6-bro/v1/audit.pdf |
| Corrected Phase 2 | 12 Dec 2024 |
| | https://github.com/cyberscope-io/audits/blob/main/6-bro/v2/audit.pdf |
| Corrected Phase 3 | 19 Dec 2024 |
| Test Deploy | https://sepolia.etherscan.io/address/0xa79442187c5F570bC49de33609A33501244adbfd |

## Source Files

| Filename | SHA256 |
| --- | --- |
| BroTokenWithPresale.sol | 87c122c29571680b815bbff7d93406a67c29d7a5c46551402f1f7c8f19f49a07 |

# Findings Breakdown

| Severity | Unresolved | Acknowledged | Resolved | Other |
|---|---|---|---|---|
| 🔴 Critical | 0 | 0 | 0 | 0 |
| 🟡 Medium | 0 | 0 | 0 | 0 |
| ⚪ Minor / Informative | 0 | 0 | 0 | 0 |

# Functions Analysis

| Contract | Type | Bases | | |
|---|---|---|---|---|
| | Function Name | Visibility | Mutability | Modifiers |
| | | | | |
| **BroTokenWithP resale** | Implementation | ERC20, ERC20Permi t, ReentrancyG uard | | |
| | | Public | ✓ | ERC20 ERC20Permit |
| | | External | Payable | - |
| | seedLP | External | ✓ | nonReentrant afterPresale notSeeded |
| | buyPresale | External | Payable | - |
| | emergencyWithdraw | External | ✓ | nonReentrant notSeeded |
| | airdropBuyers | External | ✓ | nonReentrant afterPresale seeded |
| | claimTokens | External | ✓ | nonReentrant afterPresale seeded |
| | tradingActive | Public | | - |
| | tradingRestricted | Public | | - |
| | tradingPhase | Public | | - |
| | presaleTokensPurchased | Public | | afterPresale |
| | _update | Internal | ✓ | |
| | _popAndSwapAirdrop | Private | ✓ | |

| | _beforeTokenTransfer | Private | ✓ | |
|---|---|---|---|---|
| | _buyPresale | Private | ✓ | nonReentrant notSeeded |
| | _airdrop | Private | ✓ | |
| | sendDust | Private | ✓ | |

# Inheritance Graph
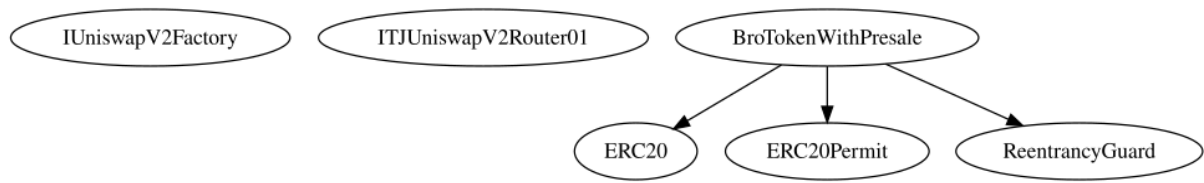
# Flow Graph
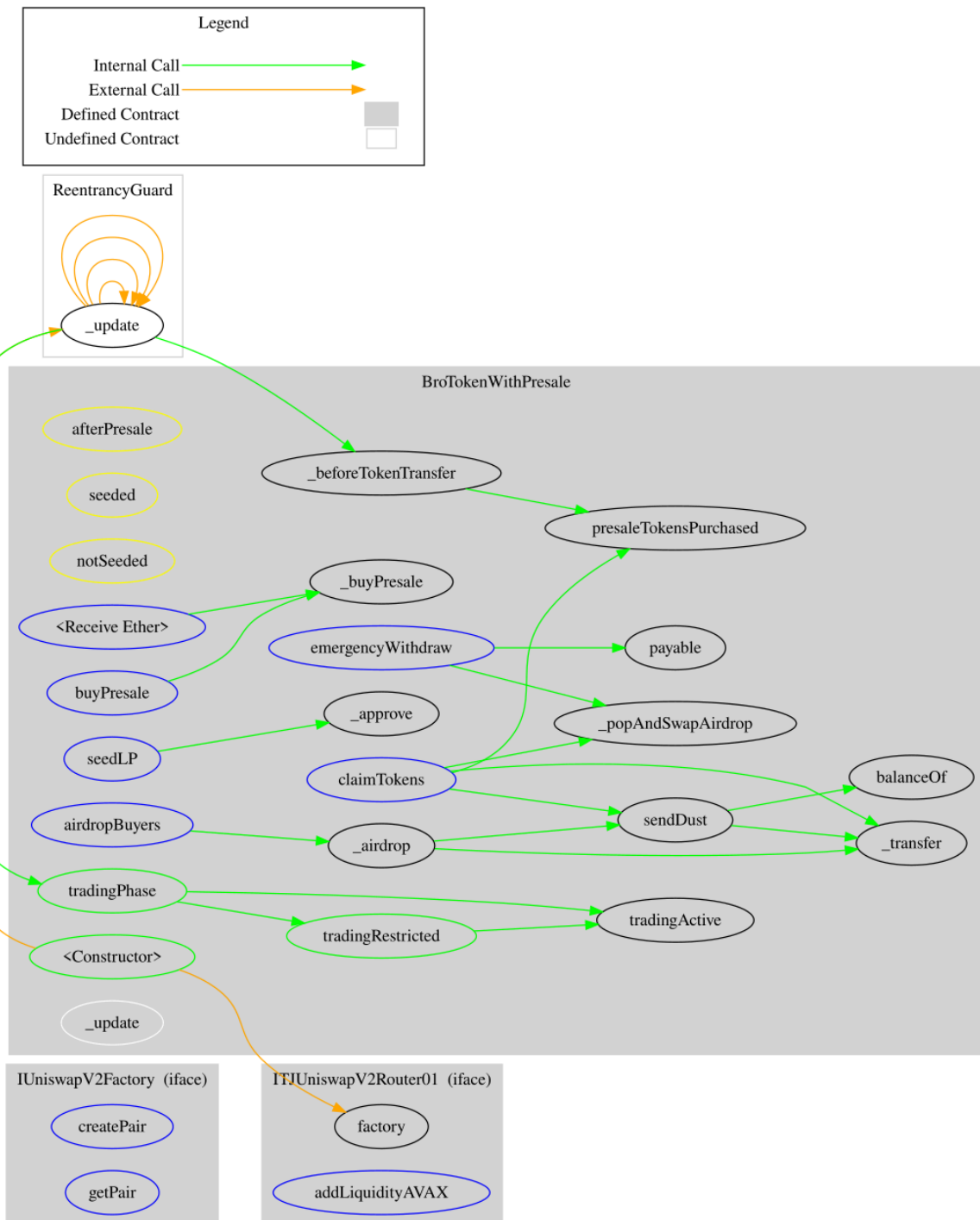
# Summary

My Bro contract implements a token and a presale mechanism. This audit investigates security issues, business logic concerns and potential improvements. My Bro is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues.

# Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

# About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

**The Cyberscope team**

cyberscope.io