CHAINPROOF

Audit Report

BANDIT

October 2024

Address : 0xE0f96F025EBB27950718ebd787b69c325CF045c0

Network : Base

Audited by © ChainProof

Table of Contents

Risk Classification

The criticality of findings in ChainProof'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.

Severity	Likelihood / Impact of Exploitation
● Critical	Highly Likely / High Impact

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.

Review

Contract Name	BanditOnBase
Initial Audit	Oct 2024 https://github.com/ChainProof-io/audits/blob/main/bandit/v1/audit.pdf
Corrected Phase 2	Oct 2024 https://github.com/ChainProof-io/audits/blob/main/bandit/v2/audit.pdf
Corrected Phase 3	Oct 2024

Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Compiler Version	v0.8.20+commit.a1b79de6
Optimization	200 runs
Explorer	https://basescan.org/address/0xe0f96f025ebb27950718ebd787b69c325cf045c0
Address	0xe0f96f025ebb27950718ebd787b69c325cf045c0
Network	BASE
Symbol	BANDIT
Decimals	18
Total Supply	10,000,000,000
Badge Eligibility	Yes

Audit Updates

Source Files

Filename	SHA256
BANDIT.sol	7fad6b341e1622d3969289f583f66833f844913d17acf35dea25eb0b6e832c1d

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

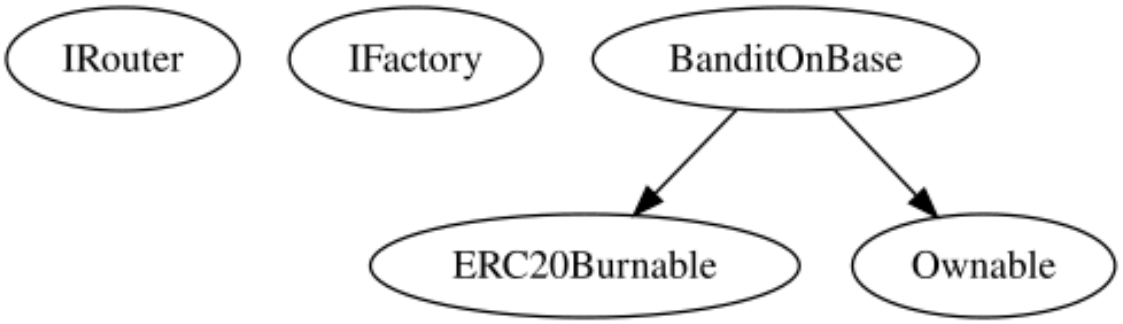
Findings Breakdown

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	0	0	0	0

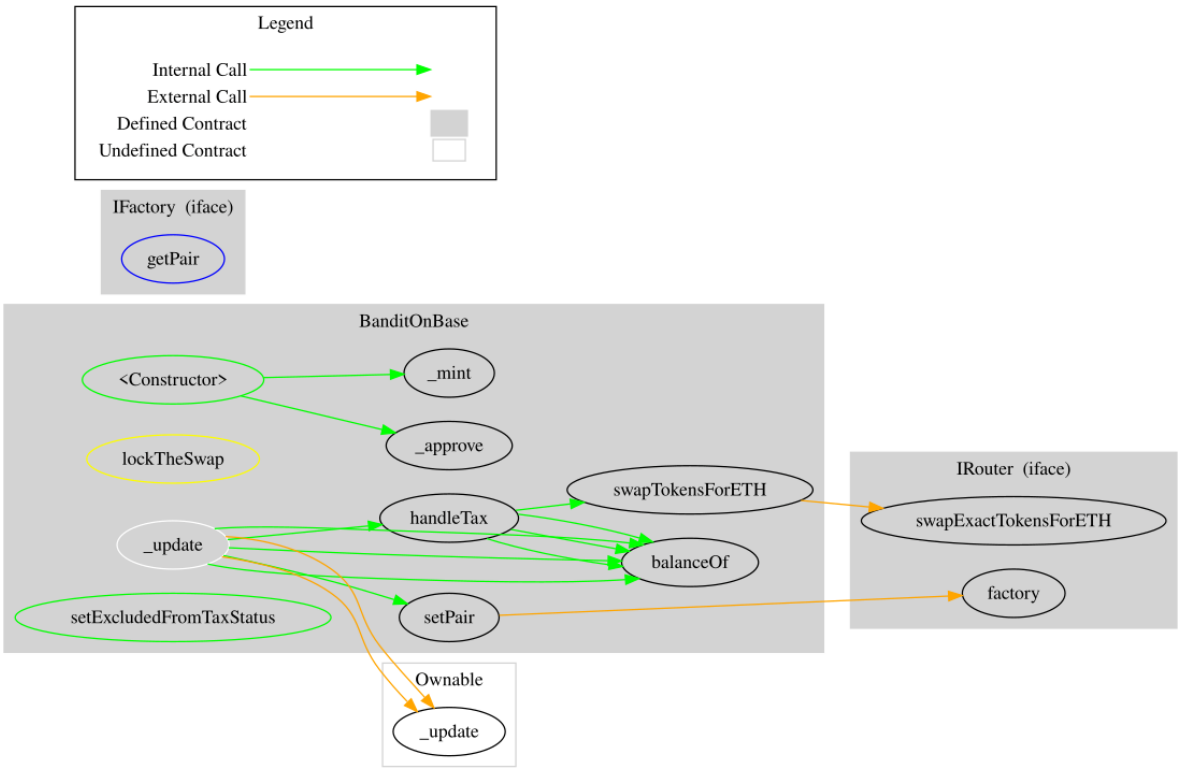
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IRouter	Interface			
	factory	External		-
	swapExactTokensForETH	External	✓	-
IFactory	Interface			
	getPair	External		-
BanditOnBase	Implementation	ERC20Burnable, Ownable		
		Public	✓	ERC20 Ownable
	_update	Internal	✓	
	handleTax	Private	✓	lockTheSwap
	swapTokensForETH	Private	✓	
	setPair	Private	✓	
	setExcludedFromTaxStatus	Public	✓	onlyOwner

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IFactory (iface)
getPair
BanditOnBase
<Constructor>
_mint
_approve
lockTheSwap
swapTokensForETH
handleTax
_update
balanceOf
setExcludedFromTaxStatus
setPair
IRouter (iface)
swapExactTokensForETH
factory
Ownable
_update

Summary

Bandit contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. Bandit is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error and no critical issues. There is also a max fee of 1% which can be automatically removed approximately 1 year from the writing of this report.

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 ChainProof’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 ChainProof 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 ChainProof’s position is that each company and individual are responsible for their own due diligence and continuous security ChainProof’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 ChainProof 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 ChainProof

Chainproof is an Audit & KYC firm for Blockchain Projects, aimed at securing the Blockchain and the assets at risk. Chainproof is fueled by Industry grade experienced Blockchain Developers from all around the globe. From finding vulnerabilities, potential scams, malicious code mitigation, improper implementation of the token which can lead to loss of user's fund, you name it and we cover and secure them all.

Security testing and risk mitigation is given the highest priority at ChainProof. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.
ChainProof is aiming to make crypto discoverable and efficient globally. We associate with extremely robust testing and code review, leaving no room for any security risks because, when it comes to user's funds, we need to leave no stone unturned. Cheers!

The ChainProof team

ChainProof.dev