Cyberscope

Audit Report

Edma

April 2025

Network	ETH
Address	0xF6fb036CA17CEeb345Fe39dFb132d1D80aB45029
Audited by	© cyberscope

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

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	CCR	Contract Centralization Risk	Acknowledged
	ISV	Inconsistent Secondary Vesting	Acknowledged
	L13	Divide before Multiply Operation	Acknowledged

Table of Contents

Analysis 1
Diagnostics 2
Table of Contents 3
Risk Classification 4
Review 5
Audit Updates 5
Source Files 6
Findings Breakdown 7
CCR - Contract Centralization Risk 8
Description 8
Recommendation 8
Team Update 9
ISV - Inconsistent Secondary Vesting 10
Description 10
Recommendation 10
Team Update 10
L13 - Divide before Multiply Operation 11
Description 11
Recommendation 11
Functions Analysis 12
Inheritance Graph 14
Flow Graph 15
Summary 16
Disclaimer 17
About Cyberscope 18

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

Contract Name	EDMA
Compiler Version	v0.8.20+commit.a1b79de6
Optimization	200 runs
Explorer	https://etherscan.io/address/0xf6fb036ca17ceeb345fe39dfb132d1d80ab45029
Address	0xf6fb036ca17ceeb345fe39dfb132d1d80ab45029
Network	ETH
Symbol	EDM
Decimals	18
Total Supply	500,000,000

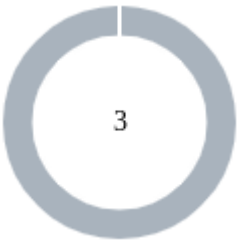
Audit Updates

Initial Audit	10 Apr 2025 https://github.com/cyberscope-io/audits/blob/main/1-edm/v1/audit.pdf
Corrected Phase 2	25 Apr 2025 https://github.com/cyberscope-io/audits/blob/main/1-edm/v2/audit.pdf
Corrected Phase 3	25 Apr 2025

Source Files

Filename	SHA256
contracts/edms/edma.sol	4b0aaf83228bbb2cb62f2564de43ff3c090e09f1262e755b9c15c1aca9d4652a

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	3

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	0	3	0	0

CCR - Contract Centralization Risk

Criticality	Minor / Informative
Location	edma.sol#L269,275
Status	Acknowledged

Description

The contract's functionality and behavior are heavily dependent on external parameters or configurations. While external configuration can offer flexibility, it also poses several centralization risks that warrant attention. Centralization risks arising from the dependence on external configuration include Single Point of Control, Vulnerability to Attacks, Operational Delays, Trust Dependencies, and Decentralization Erosion.

```
function endPresale() external onlyOwner activePresale returns
(bool){
presaleActive = false;
presaleEndTime = block.timestamp;
emit PresaleEnded(presaleEndTime);
return true;
}
```

```
function setPresale(address newPresaleAddress) external onlyOwner
activePresale validAddress(newPresaleAddress) {
emit PresaleAddressUpdated(presaleAddress, newPresaleAddress);
presaleAddress = newPresaleAddress;
}
```

Recommendation

To address this finding and mitigate centralization risks, it is recommended to evaluate the feasibility of migrating critical configurations and functionality into the contract's codebase itself. This approach would reduce external dependencies and enhance the contract's self-sufficiency. It is essential to carefully weigh the trade-offs between external configuration flexibility and the risks associated with centralization.

Team Update

Ownership of the EDMA token contract is intentionally retained during the presale period in order to facilitate essential presale operations, such as activating the vesting schedule and managing the presale address. Once the presale concludes, we will execute the `endPresale()` function, which finalizes the vesting timeline and enables full transferability. Immediately after this step, we will proceed with `renounceOwnership()` to fully decentralize the contract and eliminate any owner privileges. This approach ensures a secure, transparent, and trustless transition while maintaining the integrity of the presale process.

ISV - Inconsistent Secondary Vesting

Criticality	Minor / Informative
Location	EDMA.sol#L226
Status	Acknowledged

Description

The contract allows the vesting of tokens received from the `preSaleAddress` in multiple stages. If tokens are vested after the complete release of the previously locked balance, the released amounts from the newly vested balances are calculated proportionally to the previously locked amounts. This may result in the early release of the newly vested amount. For example, if a user receives 100 tokens that are released over the span of 5 periods, and then the user receives an additional 25 tokens, these can be released in the span of a single period. This is because the calculation of the amount to be released includes the already released balance of 100 tokens. As a result, the release schedule of new vesting periods may not follow the expected design.

```
vesting[recipient].totalLocked =  vesting[recipient].totalLocked + amount;
```

Recommendation

It is advisable to include measures that properly implement the release schedule for vested amounts at all times. This would prevent inconsistencies in the system.

Team Update

This vesting logic is intentional and part of our tokenomics design. All token allocations — not just presale — follow a vesting schedule to support long-term sustainability. Full details: docs.edma.app → Vesting Schedule (https://docs.edma.app/edma-presale/usdedm-tokenomics/vesting-schedule)

L13 - Divide before Multiply Operation

Criticality	Minor / Informative
Location	contracts/edms/edma.sol#L246,256
Status	Acknowledged

Description

It is important to be aware of the order of operations when performing arithmetic calculations. This is especially important when working with large numbers, as the order of operations can affect the final result of the calculation. Performing divisions before multiplications may cause loss of prediction.

```
uint256 intervalPassed = ((block.timestamp - presaleEndTime) /
VESTING_INTERVAL)
uint256 totalReleasable  = (vs.totalLocked * (intervalPassed * 20)) / 100
```

Recommendation

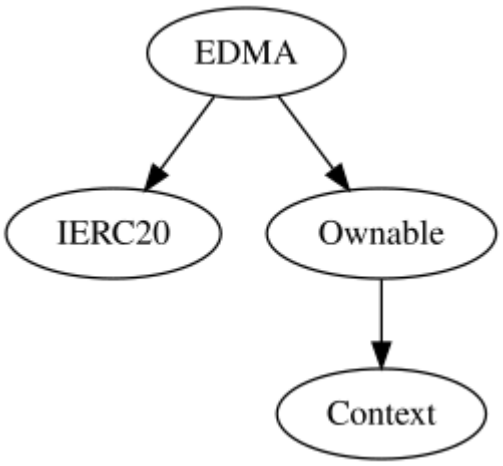
To avoid this issue, it is recommended to carefully consider the order of operations when performing arithmetic calculations in Solidity. It's generally a good idea to use parentheses to specify the order of operations. The basic rule is that the multiplications should be prior to the divisions.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
EDMA	Implementation	IERC20, Ownable		
		Public	✓	-
		External	Payable	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	burn	External	✓	-
	transferAndVest	External	✓	onlyPresale activePresale validAddress
	calculateUnlockableAmount	Public		-
	setPresale	External	✓	onlyOwner activePresale validAddress
	endPresale	External	✓	onlyOwner activePresale
	setExcludedFromVesting	External	✓	onlyOwner
	approve	Public	✓	-
	transfer	Public	✓	-

	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	recoverStuckTokens	External	✓	onlyOwner validAddress
	recoverStuckETH	External	✓	onlyOwner validAddress
	checkIfCanSpend	Internal	✓	
	_transfer	Internal	✓	validAddress validAddress
	_approve	Internal	✓	validAddress validAddress

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Custom Error Call
Defined Contract
Undefined Contract
Ownable
renounceOwnership
owner
transferOwnership
<Constructor>
onlyOwner
address
Context
_msgSender
payable
EDMA
validAddress
activePresale
<Constructor>
onlyPresale
<Receive Ether>
name
symbol
decimals
totalSupply
allowance
recoverStuckETH
setPresale
endPresale
setExcludedFromVesting
increaseAllowance
decreaseAllowance
approve
transferFrom
transfer
recoverStuckTokens
transferAndVest
_approve
burn
_transfer
checkIfCanSpend
calculateUnlockableAmount
balanceOf
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom

Summary

Edma contract implements a token and vesting mechanism. This audit investigates security issues, business logic concerns and potential improvements. 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