audita

Neo Pepe

Smart Contract Security Audit

June 16th, 2025

Prepared for:
Neo Pepe Protocol (*neopepe.ai*)

Presented By:
Audita Security (*audita.io*)

Document

The contents of this document may include confidential information pertaining to the IT systems, intellectual property, and possible vulnerabilities along with methods of exploitation that the Client may possess. The report that contains this confidential information can be utilized internally by the Client, and is made available to the public after all vulnerabilities are addressed.

Network: Ethereum, BNB, Base
Programming language: Solidity
Method: Manual Audit - Token
Client Website: https://neopepe.ai
Timeline: 15 June 2025 - 16 June 2025

Table of Contents

Audit Summary

Manual Audit

During the manual audit of the token contract conducted by our experts, we did not identify any Critical, High, Medium or Low severity vulnerabilities.

We put forward a recommendation for the team's consideration regarding the ***enableTrading()*** function - there is no mechanism to disable it when critical issues arise. Our team suggests implementing a function to disable trading operations, such as **disableTrading()**, to provide a cushion in case of an emergency and thereby enhance protocol security.

This would allow administrators to respond appropriately to potential threats or system vulnerabilities.

Overall Assessment

After a detailed and thorough security review, our researchers did not identify any notable weak links or vulnerabilities.
$NEOP token is, to the best of our knowledge, safe to use.

Severity	**Count**
Critical	0
High	0
Medium	0
Low	0
Informational	0

Documentation

We recommend this report, as well as specific information from this report to be included in Neo Pepe Protocol’s official protocol Documentation.

Audita Vulnerability Classifications

Audita follows the most recent standards for vulnerability severities, taking into consideration both the possible impact and the likelihood of an attack occurring due to a certain vulnerability.

Severity	Description
Critical	Critical vulnerability is one where the attack is more straightforward to execute and can lead to exposure of users' data, with catastrophic financial consequences for clients and users of the smart contracts.
High	The vulnerability is of high importance and impact, as it has the potential to reveal the majority of users' sensitive information and can lead to significant financial consequences for clients and users of the smart contracts.
Medium	The issue at hand poses a potential risk to the sensitive information of a select group of individual users. If exploited, it has the potential to cause harm to the client's reputation and could result in unpleasant financial consequences.
Low	The vulnerability is relatively minor and not likely to be exploited repeatedly, or is a risk that the client has indicated is not impactful or significant, given their unique business situation.
Informational	The issue may not pose an immediate threat to ongoing operation or utilization, but it's essential to consider implementing security and software engineering best practices, or employing backup measures as a safety net.

Scope

The security assessment was scoped to the Token contract in Neo Pepe’s code repository:

Files
`NeoPepe.sol`

Recommendations

Audita Security has put forward the following recommendation for Neo Pepe’s $NEOP token:

★ ***enableTrading()*** function - There is no mechanism to disable it when critical issues arise.
Our team suggests implementing a function to disable trading operations, such as **disableTrading()**, to provide a cushion in case of an emergency and thereby enhance protocol security.
This way administrators can respond appropriately to potential threats or system vulnerabilities.

Overall Assessment

After a detailed and thorough security review, our researchers did not identify any notable weak links or vulnerabilities.

$NEOP token is, to the best of our knowledge, safe to use.

Severity	**Count**
Critical	0
High	0
Medium	0
Low	0
Informational	0

Disclaimer

This audit makes no statements or warranties on the security of the code. While we have conducted the analysis to our best abilities and produced this report in line with latest industry developments, it is important to not rely on this report only. In order for contracts to be considered as safe as possible, the industry standard requires them to be checked by several independent auditing bodies. Those can be other audit firms or public bounty programs.

Smart contract platforms, their programming languages, and other software components are not immune to vulnerabilities that can be exploited by hackers. As a result, although a smart contract audit can help identify potential security issues, it cannot provide an absolute guarantee of the audited smart contract's security.