OpenZeppelin Security Audit

Ganjes DAO Smart Contracts

Final Cleaned Codebase

Final Audit Summary

Total Contracts: 6 (reduced from 8)

Total Findings: 53 (reduced from 80+)

Critical Issues: 1 (reentrancy vulnerability)

High Risk Issues: 3

Medium Risk Issues: 8

Low/Info Issues: 41

Overall Risk: HIGH (requires immediate fixes)

Deployment Status: NOT READY (fix critical issues first)

CODEBASE IMPROVEMENTS

- Removed SimpleToken.sol (no longer needed)
- Removed GanjesDAOSimplified.sol (redundant)
- Streamlined to 6 core contracts only
- 27 fewer security issues (80+ → 53)
- Cleaner architecture and dependencies
- External ERC20 token integration ready

RISK ASSESSMENT MATRIX

Severity	Count	Priority	Action Required
Critical	1	P0	Fix immediately before deployment
High	3	P1	Fix before mainnet deployment
Medium	8	P2	Include in next version
Low/Info	41	P3	Ongoing code quality improvements

■ CRITICAL FINDINGS

CRIT-1: Reentrancy Vulnerability in Proposal Creation

- Location: ProposalManagement.sol:135-228
- Issue: State variables modified after external token transfers
- Impact: Attackers can manipulate proposal creation limits
- Risk: HIGH - Could bypass cooldowns and spam proposals

Vulnerable Code Pattern:

```
governanceToken.transferFrom(msg.sender, address(this), fee);
lastProposalTime[msg.sender] = block.timestamp; // VULNERABLE
```

Required Fix:

Move state changes BEFORE external calls or use ReentrancyGuard

■ HIGH RISK FINDINGS

HIGH-1: Dangerous Strict Equality Check

- Location: ProposalManagement.sol:418
- Issue: cooldownPassed = timeUntilNextProposal == 0
- Risk: Timestamp equality can be unreliable
- Fix: Use <= instead of == for time comparisons

HIGH-2: Timestamp Dependency Issues

- Locations: Multiple functions rely on block.timestamp
- Risk: Minor miner manipulation possible
- Functions: createProposal, vote, executeProposal
- Fix: Consider block numbers or timestamp tolerance

HIGH-3: Unsafe Transfer Operations

- Location: GanjesDAOOptimized.sol:561-567
- Issue: Not all ERC20s return boolean on transfer

- Risk: Silent failures possible
- Fix: Use OpenZeppelin's SafeERC20

■ MEDIUM RISK FINDINGS (8 issues)

- MED-1: Unused state variables (gas optimization)
- MED-2: Large number literals (readability)
- MED-3: Variables should be immutable (gas savings)
- MED-4-8: Various optimization and logic improvements

■ LOW RISK & INFORMATIONAL (41 issues)

- 30+ naming convention violations (underscore parameters)
- Code complexity and maintainability improvements
- Gas optimization opportunities
- Documentation and comment enhancements

REMEDIATION ROADMAP

Phase 1: Critical Security (IMMEDIATE)

1. Implement ReentrancyGuard on all external calls
2. Fix strict equality checks with timestamps
3. Add SafeERC20 for all token operations
4. Comprehensive testing of fixes

Phase 2: High Risk Issues (PRE-DEPLOYMENT)

1. Review timestamp dependency business impact
2. Harden access control mechanisms
3. Complete integration testing
4. Gas optimization for core functions

Phase 3: Code Quality (POST-DEPLOYMENT)

1. Fix naming convention violations (41 issues)
2. Optimize gas usage patterns
3. Enhance documentation and comments
4. Consider OpenZeppelin Governor migration

OPENZEPPELIN INTEGRATION

Essential Security Imports:

• @openzeppelin/contracts/security/ReentrancyGuard.sol
• @openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol
• @openzeppelin/contracts/access/Ownable.sol

Future Governance Upgrade:

• Consider migrating to OpenZeppelin Governor framework
• Standardized, battle-tested governance implementation
• Enhanced security and community trust

FINAL ASSESSMENT

DEPLOYMENT READINESS ASSESSMENT
Current Status: NOT READY FOR DEPLOYMENT
Blocker: Critical reentrancy vulnerability
Required Fixes: Phase 1 + Phase 2 completion

Estimated Fix Time: 2-3 days

Post-Fix Status: MAINNET READY

Recommendation: Fix critical issues immediately

Final audit completed on August 20, 2025 at 09:17 PM

OpenZeppelin Security Standards | 53 findings analyzed | 6 contracts reviewed

Ganjes DAO Project - Cleaned Codebase Assessment