



Dgrid Audit Report

November 12, 2025

Dgrid Audit Report

Zero Drift

November 12, 2025

Prepared by: Zero Drift

Table of Contents

- About Zero Drift
- Disclaimer
- Risk Classification
- Protocol Overview
- Audit Scope
- Executive Summary
- Findings
 - Critical
 - High
 - Medium
 - Low
 - Informational
 - Gas

About Zero Drift

Zero Drift is a tech-driven Web3 auditing firm dedicated to zero-incident smart-contract assurance for mission-critical protocols.

Our team consists of several senior smart-contract auditors, each with 5+ years of experience and a perfect post-audit record across more than 80 successful reviews, collectively helping protect over \$5 billion in on-chain assets. We focus on the high-stakes sectors of Web3 including DEXs, lending, derivatives/perpetuals, liquid restaking, cross-chain interoperability, and stablecoins.

Disclaimer

The Zero Drift team makes all effort to find as many vulnerabilities in the code in the given time period, but holds no responsibilities for the findings provided in this document. A security audit by the team is not an endorsement of the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the Solidity implementation of the contracts.

Risk Classification

	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

Protocol Overview

Dgrid contracts (Dgrid, DgridStakePool, DgridNode, ChainlinkPriceFeed) covering node purchase and staking flows, price feed usage, per-asset/global limits, and administrative configuration.

Audit Scope

This report adapts findings from the supplied Dgrid document into Zero Drift's reporting style

Executive Summary

Summary

We reviewed administrative controls, staking lifecycle (deposit/unstake), node jailing, asset configuration and block-limit accounting, and external dependency usage. One critical issue (unstake path) and multiple high/medium/low issues were identified with clear remediations. Centralization risks are documented along with recommended event emission and validation practices.

Issues Found

	Count
Critical Risk	1
High Risk	3
Medium Risk	2
Low Risk	3
Informational	2
Gas Optimizations	0
Total Issues	11

Summary of Findings

ID	Title	Severity	Status
C-1	Deposited nodes cannot be unstaked (stake pool lacks unstake path)	Critical	Fixed

ID	Title	Severity	Status
H-1	Centralization risk: multiple owner-only mutators (rates, roles, assets, price feed, pausing, emergency withdraw)	High	Acknowledged
H-2	<code>unjailNodes</code> callable by anyone, bypassing jailing	High	Fixed
H-3	Centralized control of contract upgrade (proxy admin)	High	Acknowledged
M-1	New assets not appended to <code>assetList</code> in <code>setAssets</code>	Medium	Fixed
M-2	<code>buyNode()</code> lacks <code>msg.value</code> validation for non-native asset purchases	Medium	Fixed
L-1	<code>setRewardPerBlock</code> lacks input validation (zero address/zero rate)	Low	Fixed
L-2	Third-party dependency risk (price feed)	Low	Acknowledged
L-3	Missing zero-address validation in multiple setters	Low	Fixed

ID	Title	Severity	Status
I-1	Missing events on sensitive, centralized functions	Informational	Fixed
I-2	Missing asset binding in signed message for <code>buyNode</code>	Informational	Acknowledged

Findings

Critical

Deposited Nodes Cannot Be Unstaked

Severity: Critical — Status: Fixed

Code Location: `DgridStakePool.sol#14`

Users can deposit nodes (setting `isStaked = true`), but only `DgridStakePool` may call `DgridNode.unstake`. No function in `DgridStakePool` triggers `unstake`, so nodes remain locked and non-transferable.

Recommendation: add a controlled unstake path in `DgridStakePool` with proper access control.

High

Centralization Risk

Severity: High — Status: Acknowledged

Code Location: `Dgrid.sol#307,312,316,320,324,333,337,341,346,351`; `ChainlinkPriceFeed.sol#142,147,151`; `DgridNode.sol#120,124,128`; `DgridStakePool.sol#139,326,345,354,433,450,455,460,262`

Owner can set commission, roles, assets, price feed and parameters, pause/unpause, and emergency withdraw, etc.

Recommendation: constrain with time-locks/multisig, emit events, and document governance processes.

Centralized Control of Contract Upgrade

Severity: High — Status: Acknowledged

Code Location: Dgrid.sol#14; DgridNode.sol#8; DgridStakePool.sol#14

`admin` can update the implementation behind the proxy for Dgrid, DgridNode and DgridStakePool. If the `admin` key is compromised, a malicious implementation could be set.

Recommendation: reduce upgrade centralization with multisig + timelock; monitor and emit events; consider delay and on-chain review process.

unjailNodes Unrestricted

Severity: High — Status: Fixed

Code Location: DgridStakePool.sol#294

Anyone could call `unjailNodes` to revert jailing by the server.

Recommendation: restrict via `onlyServer`/signature verification.

Resolution: Signature verification added to `unjailNodes`.

Medium

New Assets Are Not Added to `assetList`

Severity: Medium — Status: Fixed

Code Location: Dgrid.sol#324

`setAssets` updates `assetInfos` but does not append new assets to `assetList`, causing iteration discrepancies.

Recommendation: push new assets into `assetList` if missing.

Lack of Validation for `msg.value` in `buyNode()`

Severity: Medium — Status: Fixed

Code Location: Dgrid.sol#178

`buyNode()` fails to enforce `msg.value == 0` when purchasing with non-native assets, risking accidental value loss.

Recommendation: add `require(msg.value == 0)` when `asset != address(0)`.

Resolution: Removed `payable` modifier from `buyNode()`.

Low

setRewardPerBlock Lacks Validation

Severity: Low — Status: Fixed

Code Location: DgridStakePool.sol#326

Missing checks for non-zero reward token and positive rate.

Recommendation: validate inputs before state changes.

Third-Party Dependencies

Severity: Low — Status: Acknowledged

Code Location: Dgrid.sol#24

External price feed assumptions; monitor oracle behavior and add failsafes.

Missing Zero Address Validation

Severity: Low — Status: Fixed

Code Location: Dgrid.sol#307,312,316; DgridNode.sol#120,124; DgridStakePool.sol#354

Add zero-address checks to setter inputs.

Informational

Missing Emit Events

Severity: Informational — Status: Fixed

Code Location: Dgrid.sol#307,312,316,320,324,333,337; ChainlinkPriceFeed.sol#142,147,151; DgridNode.sol#120,124,128; DgridStakePool.sol#139,326,345,354

Emit events for sensitive, centralized operations for traceability.

Missing Asset Binding in Signed Message for buyNode

Severity: Informational — Status: Acknowledged

Code Location: Dgrid.sol#110

The `buyNode` verification message signed by the trusted server does not bind the `asset` address. A user could specify a different asset from `assetInfos` than the one intended in the signed message.

Recommendation: include the [asset](#) address in the signed payload to bind the instruction to a specific token; validate on-chain before processing.

Gas

No gas optimization items tracked.