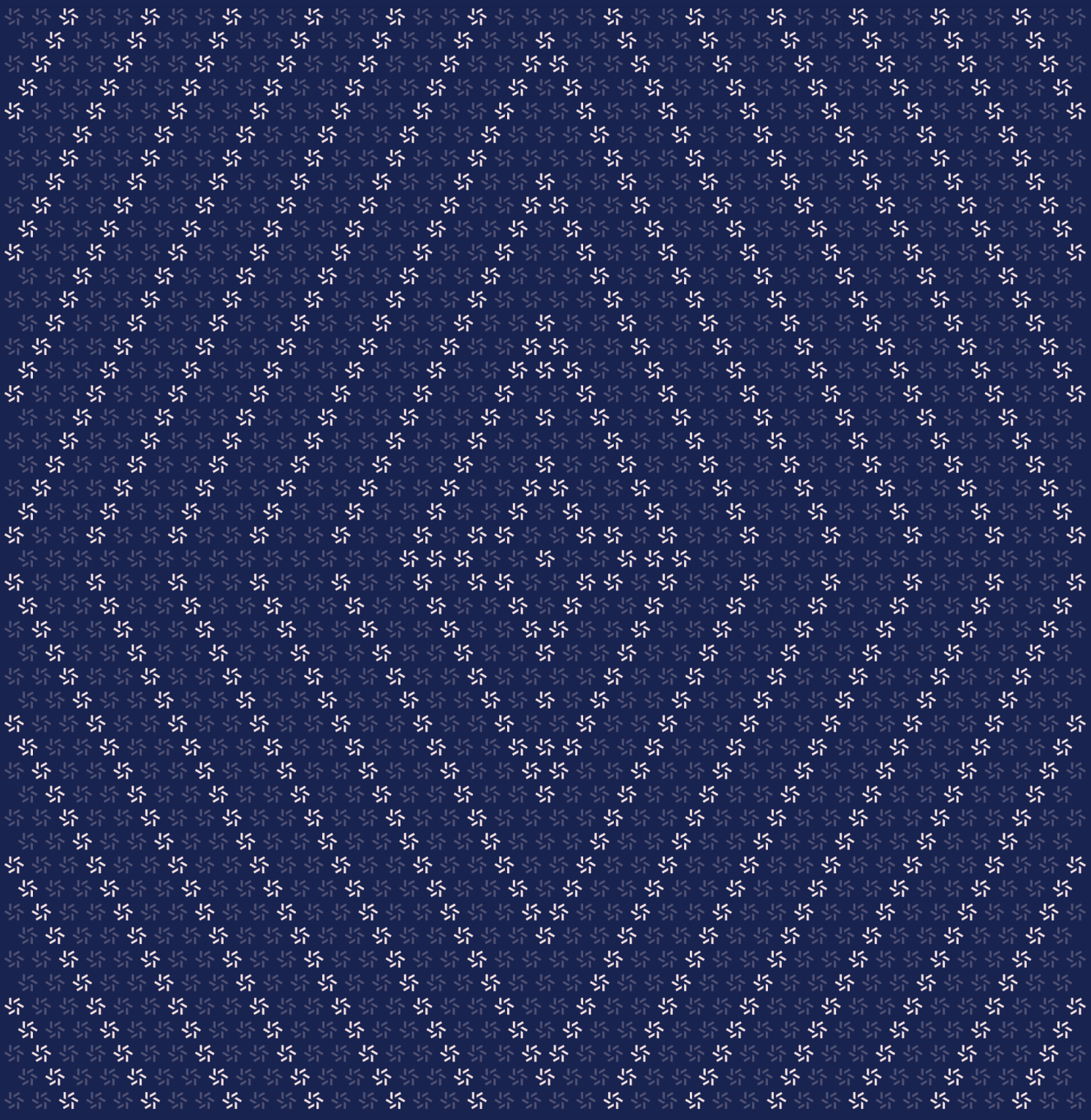
Zellic

Prepared for
Hein Dauven
Dusk Network B.V.

Prepared by
Qingying Jie
Juchang Lee
Zellic

October 9, 2024

Migration
Smart Contract Security Assessment



Contents

About Zellic

Zellic is a vulnerability research firm with deep expertise in blockchain security. We specialize in EVM, Move (Aptos and Sui), and Solana as well as Cairo, NEAR, and Cosmos. We review L1s and L2s, cross-chain protocols, wallets and applied cryptography, zero-knowledge circuits, web applications, and more.

Prior to Zellic, we founded the #1 CTF (competitive hacking) team ↗ worldwide in 2020, 2021, and 2023. Our engineers bring a rich set of skills and backgrounds, including cryptography, web security, mobile security, low-level exploitation, and finance. Our background in traditional information security and competitive hacking has enabled us to consistently discover hidden vulnerabilities and develop novel security research, earning us the reputation as the go-to security firm for teams whose rate of innovation outpaces the existing security landscape.

For more on Zellic's ongoing security research initiatives, check out our website zellic.io ↗ and follow @zellic_io ↗ on Twitter. If you are interested in partnering with Zellic, contact us at hello@zellic.io ↗.

1. Overview

1.1. Executive Summary

Zellic conducted a security assessment for Dusk Network B.V. from October 4th to October 7th, 2024. During this engagement, Zellic reviewed Migration's code for security vulnerabilities, design issues, and general weaknesses in security posture.

1.2. Goals of the Assessment

In a security assessment, goals are framed in terms of questions that we wish to answer. These questions are agreed upon through close communication between Zellic and the client. In this assessment, we sought to answer the following questions:

- Could malicious users exploit the contract through reentrancy attacks?
- Is the rounding mechanism handled correctly?
- Is there a risk of token loss during the transfer?
- Is the migration contract working as expected?

1.3. Non-goals and Limitations

We did not assess the following areas that were outside the scope of this engagement:

- Front-end components
- Infrastructure relating to the project
- Key custody

Due to the time-boxed nature of security assessments in general, there are limitations in the coverage an assessment can provide.

1.4. Results

During our assessment on the scoped Migration contracts, there were no security vulnerabilities discovered.

Zellic recorded its notes and observations from the assessment for the benefit of Dusk Network B.V. in the Discussion section (3. ↗).

Breakdown of Finding Impacts

Impact Level	Count
Critical	0
High	0
Medium	0
Low	0
Informational	0

2. Introduction

2.1. About Migration

Dusk Network B.V. contributed the following description of Migration:

> The DUSK migration contract is used for migrating ERC20/BEP20 DUSK to native DUSK.

2.2. Methodology

During a security assessment, Zellic works through standard phases of security auditing, including both automated testing and manual review. These processes can vary significantly per engagement, but the majority of the time is spent on a thorough manual review of the entire scope.

Alongside a variety of tools and analyzers used on an as-needed basis, Zellic focuses primarily on the following classes of security and reliability issues:

Basic coding mistakes. Many critical vulnerabilities in the past have been caused by simple, surface-level mistakes that could have easily been caught ahead of time by code review. Depending on the engagement, we may also employ sophisticated analyzers such as model checkers, theorem provers, fuzzers, and so on as necessary. We also perform a cursory review of the code to familiarize ourselves with the contracts.

Business logic errors. Business logic is the heart of any smart contract application. We examine the specifications and designs for inconsistencies, flaws, and weaknesses that create opportunities for abuse. For example, these include problems like unrealistic tokenomics or dangerous arbitrage opportunities. To the best of our abilities, time permitting, we also review the contract logic to ensure that the code implements the expected functionality as specified in the platform's design documents.

Integration risks. Several well-known exploits have not been the result of any bug within the contract itself; rather, they are an unintended consequence of the contract's interaction with the broader DeFi ecosystem. Time permitting, we review external interactions and summarize the associated risks: for example, flash loan attacks, oracle price manipulation, MEV/sandwich attacks, and so on.

Code maturity. We look for potential improvements in the codebase in general. We look for violations of industry best practices and guidelines and code quality standards. We also provide suggestions for possible optimizations, such as gas optimization, upgradability weaknesses, centralization risks, and so on.

For each finding, Zellic assigns it an impact rating based on its severity and likelihood. There is no hard-and-fast formula for calculating a finding's impact. Instead, we assign it on a case-by-case basis based on our judgment and experience. Both the severity and likelihood of an issue affect its impact. For instance, a highly severe issue's impact may be attenuated by a low likelihood. We assign the following impact ratings (ordered by importance): Critical, High, Medium, Low, and

Informational.

Zellic organizes its reports such that the most important findings come first in the document, rather than being strictly ordered on impact alone. Thus, we may sometimes emphasize an "Informational" finding higher than a "Low" finding. The key distinction is that although certain findings may have the same impact rating, their *importance* may differ. This varies based on various soft factors, like our clients' threat models, their business needs, and so on. We aim to provide useful and actionable advice to our partners considering their long-term goals, rather than a simple list of security issues at present.

Finally, Zellic provides a list of miscellaneous observations that do not have security impact or are not directly related to the scoped contracts itself. These observations — found in the Discussion (3. ↗) section of the document — may include suggestions for improving the codebase, or general recommendations, but do not necessarily convey that we suggest a code change.

2.3. Scope

The engagement involved a review of the following targets:

Migration Contracts

Type	Solidity
Platform	EVM-compatible
Target	dusk-migration
Repository	https://github.com/dusk-network/dusk-migration ↗
Version	`e0826ab95be5fae319276a3449418ce040499d7e`
Programs	`contracts/DUSKMigration.sol`

2.4. Project Overview

Zellic was contracted to perform a security assessment for a total of one person-day. The assessment was conducted by two consultants over the course of two calendar days.

Contact Information

The following project managers were associated with the engagement:

Jacob Goreski
Engagement Manager
jacob@zellic.io

Chad McDonald
Engagement Manager
chad@zellic.io

The following consultants were engaged to conduct the assessment:

Qingying Jie
Engineer
qingying@zellic.io

Juchang Lee
Engineer
lee@zellic.io

2.5. Project Timeline

The key dates of the engagement are detailed below.

October 4, 2024	Start of primary review period
October 7, 2024	End of primary review period

3. Discussion

The purpose of this section is to document miscellaneous observations that we made during the assessment. These discussion notes are not necessarily security related and do not convey that we are suggesting a code change.

3.1. The code comments for the function `migrate`

The comments for the function `migrate` mention that the function follows the checks-effects-interactions pattern (CEI) and list which step each operation corresponds to.

```
* @dev This function uses the check-effects-interactions pattern to mitigate
    reentrancy risks.
    External calls are only made after internal state changes. Specifically:
* 1. Check: Check if the `amount` is greater than or equal to 1 LUX.
* 2. Effect: Transfers the specified amount of DUSK tokens from the sender to
    the contract.
* 3. Interaction: Emits a `Migration` event,
    which is being relied upon for issuing native DUSK.
```

In fact, in the CEI pattern, "effects" refer to operations that update the state variables of the current contract, while "interactions" refer to operations that interact with external contracts. Therefore, the token transfer should correspond to the interactions step. Since the function does not involve updating state variables, the function `migrate` has no effects.

This issue has been acknowledged by Dusk Network B.V., and a fix was implemented in commit 54077dbe ↗.

4. Threat Model

This provides a full threat model description for various functions. As time permitted, we analyzed each function in the contracts and created a written threat model for some critical functions. A threat model documents a given function's externally controllable inputs and how an attacker could leverage each input to cause harm.

Not all functions in the audit scope may have been modeled. The absence of a threat model in this section does not necessarily suggest that a function is safe.

4.1. Module: DUSKMigration.sol

Function: `migrate(uint256 amount, string memory targetAddress)`

This function migrates ERC-20 DUSK tokens to native DUSK.

Inputs

- `amount`
  - **Control**: Fully controlled by the caller.
  - **Constraints**: Must be at least 1 LUX (10^9 WEI).
  - **Impact**: The amount of ERC-20 DUSK tokens to migrate in DUSK WEI.
- `targetAddress`
  - **Control**: Fully controlled by the caller, but basically, it will be provided by the UX.
  - **Constraints**: N/A.
  - **Impact**: N/A.

Branches and code coverage

Intended branches

- Check if `amount` is at least 1 LUX.
  - ☑ Test coverage
- Get the round-down amount to the nearest multiple of 1 LUX.
  - ☑ Test coverage
- Transfer the round-down amount to the contract.
  - ☑ Test coverage

Negative behavior

- The `amount` is smaller than 1 LUX.
  - ☑ Negative test

5. Assessment Results

At the time of our assessment, the reviewed code was not deployed to the Ethereum Mainnet.

During our assessment on the scoped Migration contracts, there were no security vulnerabilities discovered.

5.1. Disclaimer

This assessment does not provide any warranties about finding all possible issues within its scope; in other words, the evaluation results do not guarantee the absence of any subsequent issues. Zellic, of course, also cannot make guarantees about any code added to the project after the version reviewed during our assessment. Furthermore, because a single assessment can never be considered comprehensive, we always recommend multiple independent assessments paired with a bug bounty program.

For each finding, Zellic provides a recommended solution. All code samples in these recommendations are intended to convey how an issue may be resolved (i.e., the idea), but they may not be tested or functional code. These recommendations are not exhaustive, and we encourage our partners to consider them as a starting point for further discussion. We are happy to provide additional guidance and advice as needed.

Finally, the contents of this assessment report are for informational purposes only; do not construe any information in this report as legal, tax, investment, or financial advice. Nothing contained in this report constitutes a solicitation or endorsement of a project by Zellic.