

Blackthorn

Security Review For Morpho

Collaborative Audit Prepared For: **Morpho**

Lead Security Expert(s): **0x73696d616f**

hyh

pkqs90

xiaoming90

Date Audited: **April 6 - April 22, 2026**

Introduction

MidnightBundlesV1 contract provides opinionated entries for the Midnight fixed-rate lending protocol.

Scope

Initial

- Audited Commit: 8de7076fb1edd52c39694ba09c65f6bbef2a9c25
- Repository: morpho-org/midnight

Files:

- src/periphery/MidnightBundles.sol
- src/periphery/interfaces/IMidnightBundles.sol

Final (signed off by Blackthorn)

- Final Commit: 55bcda615e4b05acec958f16e58c681ca750a0bb
- Repository: morpho-org/bundles

Files:

- src/midnight/MidnightBundlesV1.sol
- src/midnight/interfaces/IMidnightBundlesV1.sol

Final Commit Hash:

55bcda615e4b05acec958f16e58c681ca750a0bb

Findings

Each issue has an assigned severity:

- High issues are directly exploitable security vulnerabilities that need to be fixed.

- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
- Low/Info issues are non-exploitable, informational findings that do not pose a security risk or impact the system's integrity. These issues are typically cosmetic or related to compliance requirements, and are not considered a priority for remediation.

Low/Informational Severity Findings: 1

Issues Not Fixed and Not Acknowledged

High	Medium	Low/Info
0	0	0

Security Experts Dedicated to This Review

@0x73696d616f

A stylized handwritten signature in white ink. It features a large, circular loop on the left side, with a diagonal stroke crossing through it. The name "Simao" is written in a cursive script to the right of the loop.

@hyh

A handwritten signature in white ink. It consists of the letters "hyh" written in a fluid, cursive style. The "h" is tall and has a long, sweeping tail that extends to the right.

@pkqs90

A handwritten signature in white ink. It is a highly stylized, cursive signature. The letters "pkqs90" are integrated into a complex, flowing script with many loops and flourishes.

@xiaoming90

A handwritten signature in white ink. It features the name "Xiaoming90" written in a cursive script. The "X" is large and has a long, horizontal stroke extending to the left. The "90" is written at the end of the signature.

Issue L-1: midnight parameter in MidnightBundles could be set in the constructor [RESOLVED]

Source:

<https://github.com/sherlock-audit/2026-04-morpho-midnight-apr-6th-2026/issues/42>

Summary

Every external function in `MidnightBundles` accepts `midnight` as a caller supplied parameter, which is not needed and could be set in the constructor instead for better phishing resistance.

Vulnerability Detail

The bundler uses the supplied `midnight` for three operations in the same call:

1. The auth gate: `IMidnight(midnight).isAuthorized(taker, msg.sender)`.
2. Approval: `_forceApproveMax(token, midnight)`.
3. External dispatch: `IMidnight(midnight).take(...) / repay / supplyCollateral / withdrawCollateral`.

A phishing frontend, malicious SDK, or compromised wallet induces the victim to call the bundler with `midnight = EvilMidnight`, and allows token theft bypassing the checks above.

Impact

Theft of all tokens pulled in a single call, bounded by the user's signed permit amount or approval.

Code Snippet

https://github.com/sherlock-audit/2026-04-morpho-midnight-apr-6th-2026/blob/main/morpho-org__midnight/src/periphery/MidnightBundles.sol#L306-L326

For example:

```
function repayAndWithdrawCollateral(
    address midnight,
    Market memory market,
    uint256 assets,
    address onBehalf,
    TokenPermit memory loanTokenPermit,
    ...
) external {
    require(onBehalf == msg.sender || IMidnight(midnight).isAuthorized(onBehalf,
        ↪ msg.sender), Unauthorized());
    ...
    _pullToken(loanToken, msg.sender, assets, loanTokenPermit);
    _forceApproveMax(loanToken, midnight);

    IMidnight(midnight).repay(market, units, onBehalf, address(0), "");
    ...
}
```

The same pattern repeats at lines 38, 106, 170, and 243.

Tool Used

Manual Review

Recommendation

Hardcode `midnight` as an `immutable` set in the constructor and remove the parameter from every external function. This mirrors how `EcrecoverRatifier` already pins its `MIDNIGHT`:

```
address public immutable MIDNIGHT;
```

```
constructor(address midnight) {  
    MIDNIGHT = midnight;  
}
```

Discussion

MathisGD

fixed in <https://github.com/morpho-org/midnight/pull/886>

Disclaimers

Blackthorn does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.