Appendix A - Bug Disclosure
NM-0534 Lagoon

NETHERMIND
SECURITY

(January 22, 2026)

Appendix A

This appendix serves as a supplement to the Security Review completed on May 13, 2025. Following the conclusion of the initial assessment, the Lagoon team identified an additional finding during continued code analysis.

This appendix describes the technical details of the new finding and the steps the Lagoon team will take to resolve it.

Finding description

[Low] The `updateRates(...)` function allows bypassing the fee update cooldown

File(s): `src/v0.5.0/FeeManager.sol`

Description: The `updateRates(...)` function allows the contract owner to update fee parameters. To prevent immediate changes, the system imposes a cooldown period during which the protocol should continue using the old rates. This is implemented by storing the previous rates in `oldRates` and the new rates in `rates`, with a timestamp determining which one is returned by `feeRates()`.

However, the `updateRates(...)` function updates the `rates` storage slot immediately with the new value. If the owner calls `updateRates(...)` twice in succession, the second call reads the `rates` slot (which now holds the new rates from the first call) and assigns it to `oldRates`.

```
function updateRates(Rates memory newRates) external onlyOwner {
    FeeManagerStorage storage $ = _getFeeManagerStorage();
    // ...

    uint256 newRatesTimestamp = block.timestamp + $.cooldown;
    // @audit-issue Reads raw storage. If called twice, this reads the 'future' rates set
    // in the first call.
    Rates memory currentRates = $.rates;

    $.newRatesTimestamp = newRatesTimestamp;
    // @audit The new rates are now set as the 'old' rates, making them active immediately.
    $.oldRates = currentRates;
    $.rates = newRates;

    emit RatesUpdated(currentRates, newRates, newRatesTimestamp);
}
```

This allows the owner to bypass the intended cooldown mechanism and make fee changes effective immediately.

Recommendation(s): Consider updating the logic to ensure that consecutive updates cannot bypass the cooldown period.

Status: Acknowledged.

Update from the client: This issue will be addressed in a future update. Currently, no action will be taken as it does not represent an immediate threat to the protocol.