

Contracts vulnerabilities

Vulnerabilities list: #1

Contracts vulnerabilities	1
Vulnerabilities list: #1	1
Involved contracts and level of the bugs	1
Vulnerabilities	1
1. <code>getPastVotes</code> vulnerability	1
2. <code>balanceOfAt</code> vulnerability	2
3. <code>_checkpoint</code> vulnerability	3
4. <code>createLockFor</code> vulnerability	4
5. <code>totalSupplyLockedAtT</code> vulnerability	5
6. <code>getPastTotalSupply</code> vulnerability	5

Involved contracts and level of the bugs

The present document aims to point out some vulnerabilities in the contracts veOLAS, buOLAS. Some of these vulnerabilities may lead to critical¹ bugs.

Vulnerabilities

1. `getPastVotes` vulnerability

Acknowledgments: This vulnerability was discovered thanks to [howd4ys](#) who kindly reported it by participating in the [Autonolas Immunefi Bug Program](#).

Severity: Low²

In the veOLAS contract, the following function is implemented:

```
function getPastVotes(address account, uint256 blockNumber) public  
view override returns (uint256 balance)
```

This function returns the voting power of the address `account` at a specific `blockNumber`.

¹ The level of the bug is assigned by following the [Immunefi classification](#)

² Since no manipulation of governance voting can currently happen, this vulnerability identifies a smart contract that fails to deliver promised returns but doesn't lose value.

This function has an incorrect behavior when the input `blockNumber` is smaller than the block number `n` where a lock was first created for the `account`.

Specifically, denoting by T the timestamp of the input `blockNumber` and T_1 the timestamp of the block `n`, the incorrect behavior arises because of the subtraction [veOLAS.sol#L680](#) that becomes an addition when `blockTime=T` is smaller than `uPoint.ts=T1`. Denoting by T_2 the `endTime` for the locking created for the `account` at time T_1 , the calculation in [veOLAS.sol#L680](#) provides the following value for the bias $\text{bias} = \text{slope} * (T_2 - T)$. However, the latter bias is bigger than the correct value for the bias at the timestamp T_1 which should be $\text{slope} * (T_2 - T_1)$.

We recommend using as an input parameter of the function a `blockNumber` bigger than the block number `n` where a lock was first created for the `account`.

Note that the function `getPastVotes(account, blockNumber)` is used to weigh the voting power of users that cast a vote on a governance proposal. Whether there is a governance proposal and a user creates a lock after the beginning and no later than the end of the voting period, due to this vulnerability of `getPastVotes(account, blockNumber)`, the user would be able to cast a voting power bigger than its correct one. Note that the manipulation of the voting power has an upper bound due to the fact that there is a limited number of blocks in a voting period and that any locks last at least one week. Nevertheless, currently, there is no possibility of creating new locks, so this issue cannot affect any governance voting.

The wrapped veOLAS (wveOLAS) contract wraps original veOLAS view functions and serves as mitigating measures to address this issue.

2. `balanceOfAt` vulnerability

Severity: Low³

In the veOLAS contract, the following function is implemented:

```
function balanceOfAt(address account, uint256 blockNumber) external  
view returns (uint256 balance)
```

This function returns the actual balance of the address `account` at a specific `blockNumber`.

³ This function is not currently used in any of the Autonolas on-chain contracts, thus this vulnerability identifies a smart contract that fails to deliver promised returns but doesn't lose value.

This function has an incorrect behavior when the input `blockNumber` is smaller than the block number `n` where a lock was first created for the `account`.

As for the previous vulnerability explanation (`getPastVotes()`), the function `balanceOfAt()` uses the same binary search algorithm followed by identical value extraction, and thus returns a very first balance of a locked point, whereas it should return zero.

We recommend using `blockNumber` input parameter value bigger than the block number `n` where a lock was first created for the `account`.

The wrapped veOLAS (wveOLAS) contract wraps original veOLAS view functions and serves as mitigating measures to address this issue.

3. `_checkpoint` vulnerability

Severity: Medium⁴

In the veOLAS contract, the following function is implemented:

```
function _checkpoint(address account, LockedBalance memory oldLocked,
LockedBalance memory newLocked, uint128 curSupply) internal
```

According to the article on medium.com, the declaration of a memory struct *lastPoint* and its assignment to another memory struct leads to the pointer of the initial struct, and not its deep copy, that can be observed in line [219](#). This leads to the incorrect calculations of history points for the periods of time when there was no *checkpoint()* function called for more than a week.

This behavior leads to the creation of supply points that have an incorrect block number which is detached from the actual timestamp. This further leads to the scenario where all supply points during the weeks of inactivity of veOLAS have the same block numbers as the first point that triggered the *checkpoint()*. In other words, all the supply points that were recreated for the weekly periods of veOLAS inactivity will not be correctly recovered during the block number search (via the block number itself or the timestamp). Any historic lookups between two supply points (not including points themselves) that were created in the *_checkpoint()* function with more than a week of inactivity will have an incorrect block number equal to the one of a first point.

⁴ When voting via veOLAS, the incorrect value is returned as a read-only value, thus this could be declared as a Low severity. However, if there are consequences due to incorrect voting failure, then it is a potential damage to the DAO members, and then the severity is Medium.

This might potentially affect the voting functionality. If the voting was performed during the time that had to account for the inactivity weeks, the weighted total supply (the overall number of votes) in the function *getPastTotalSupply()* might return incorrect values (depending on the first point with the same block number found via a binary search).

In the absence of deploying new contracts, we recommend running the analogue of the cron scheduler / service that checks for the veOLAS activity during the week, and if there was none, trigger a *checkpoint()* function call. This way, all the supply points will be correctly updated throughout the time of the contract. As the protocol becomes more active, this issue will resolve itself by the participation of DAO members.

4. `createLockFor` vulnerability

Severity: Medium

In veOLAS and buOLAS contracts, the following function is implemented:

```
function createLockFor(address account, uint256 amount, uint256
unlockTime) external
```

This function allows anyone, even a smart contract, to create a lock for a third-party account. If the third-party account has already a locked amount the call will be reverted. If not and the OLAS amount provided as input is non-zero then a lock is created. As a consequence, any third-party account can be forced into a long lock length (for a maximum of 4 years for veOLAS and 10 years for buOLAS) by an attacker calling ``createLockFor`` with a very small amount of OLAS (i.e. $1/10^{18}$) and a max lock length. An attacker could use this to prevent locks over a given adversarially chosen interval by front-running all locks in this manner. All accounts with an intent to lock for less than 4 years would be affected.

We assign a low likelihood to this attack, as it is not economically profitable for the attacker.

Indeed, the caller of the ``createLockFor`` function can lock for third-party users only by using its own OLAS tokens. So the mintable OLAS tokens can be temporarily frozen only with an attacker's extensive cost.

In the buOLAS contract, there is also an extra guardrail that can be considered. If the attack has been discovered, it is possible to invoke a governance vote to revoke the unvested OLAS of the third-party account that has been forced in a long lock into buOLAS. If the governance approves the revoke, the third-party account can call the

buOLAS withdraw function, and all non-vested OLAS tokens will be burned. When the withdraw function is called less than one year after the attack, all the contract status can return to their original status before the attack has been made.

5. `totalSupplyLockedAtT` vulnerability

Severity: Low

In the veOLAS contract, the following function is implemented:

```
function totalSupplyLockedAtT(uint256 ts) public view returns
(uint256)
```

The function is used solely by the `totalSupplyLocked()` function with the current `block.timestamp`. By the original design, it is not intended to have a `ts` parameter smaller than the current `block.timestamp`.

We recommend not to call this function for any external purposes. It is a view function that is not currently used externally in any of Autonolas on-chain protocol contracts, and thus does not affect any intended behavior.

The wrapped veOLAS (wveOLAS) contract wraps original veOLAS view functions and serves as mitigating measures to address this issue.

6. `getPastTotalSupply` vulnerability

Severity: Low

In the veOLAS contract, the following function is implemented:

```
function getPastTotalSupply(uint256 blockNumber) external view
returns (uint256)
```

The function returns the voting power of a specified block number. However, by the original implementation, the requested block number must be at least equal to the zero supply point block number, or the block number of a contract deployment. Otherwise, the function reverts instead of returning a zero value.

We recommend not to call this function with the input block number value less than a zero supply point block number, since it is meaningless anyway as there must be no values before the very first supply point is created in the contract.