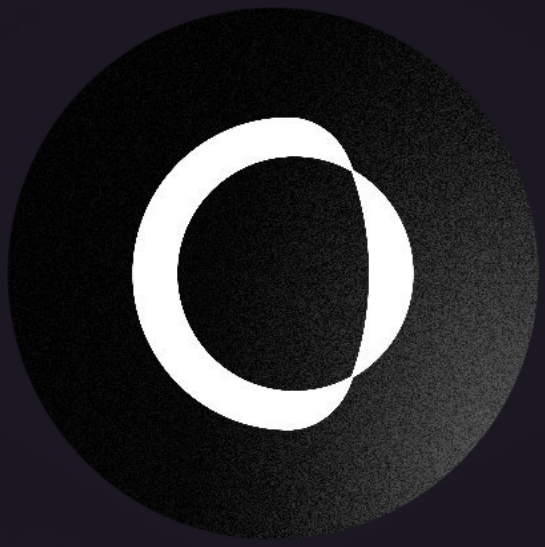
SHERLOCK

Security Review For Usual



Collaborative Audit Prepared For: **Usual**
Lead Security Expert(s): **0x73696d616f**
xiaoming90
Date Audited: **December 29 - December 30, 2025**

Introduction

The security review focused on the deprecation of features by removal of logic, specifically the auto-staking of Usual for UsualSP holders towards UsualX.

Scope

Repository: usual-dao/core-protocol

Audited Commit: a2023fab70847dc6c1a9c000389ce503b4d111ae

Final Commit: a2023fab70847dc6c1a9c000389ce503b4d111ae

Files:

- scripts/deployment/P26.s.sol
- src/interfaces/token/IUsualSP.sol
- src/token/UsualSP.sol

Final Commit Hash

a2023fab70847dc6c1a9c000389ce503b4d111ae

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.

Issues Found

High	Medium	Low/Info
0	0	0

Issues Not Fixed and Not Acknowledged

High	Medium	Low/Info
0	0	0

Auditors' note

The security review focused on the deprecation of features by removal of logic, specifically the auto-staking of Usual for UsualSP holders towards UsualX.

Two main key features were checked against:

- Sweep of the accumulated Usual still emitted on the UsualSP contract:
  - Capabilities by the USUALSP_OPERATOR to sweep the emitted Usual towards an account for management.
  - Removal of the auto-stacking by ceasing to deposit Usual into UsualX.
- Role-based Access Control: Restricts critical operations to authorized roles.
- Core Functionalities:
  - Accumulation of Usual on UsualSP contract:
  - Automatic daily process
- Sweeping of accumulated Usual on UsualSP contract:
  - Restricted by Role Base Access Control (USUALSP_OPERATOR)
- Access Control and Upgradeability:
  - Role-based permissions restrict critical actions (e.g., minting, oracle updates).
  - Contracts utilize OpenZeppelin's upgradeable patterns.

Key Areas of Focus:

- Economic issues: Confirming that flashloaning/flashminting does not expose the protocol to systemic issues.
- Role-Based Permissions: Confirming that only authorized roles can execute critical operations.
- Emergency Mechanisms: Ensuring robust and proper implementation of pause/unpause functionalities.
- Precision and Math Safety: Verifying correctness and safety in all calculations, especially for price normalization and conversion.
- Upgradeability: Validating secure initialization and upgrades to prevent unauthorized modifications.

Disclaimers

Sherlock 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.