[RFC] - Adopt The SEAL Safe Harbor Agreement

Category: Request for comment

Authors: Skylock.xyz, @eek637

Introduction

This proposal outlines Uniswap Governance's adoption of the SEAL (Security Alliance) Whitehat Safe Harbor Agreement ("Safe Harbor Agreement"). By adopting Safe Harbor, Uniswap improves the security of its on-chain assets by allowing whitehats to intervene during active exploits to save protocol funds.

What is the Safe Harbor Agreement?

The Safe Harbor Agreement addresses a critical need in crypto: enabling whitehats to intervene during active exploits when traditional responsible disclosure procedures are not feasible.

Key aspects of the agreement include:

- Encouraging Whitehats to Protect the Protocol: By adopting Safe Harbor, Uniswap incentivizes whitehats to step in and protect the protocol during active exploits by limiting their legal exposure.

- Intervention Only During Active Exploits: Whitehats are authorized to act only when there is an immediate or ongoing exploit that threatens the protocol. This agreement applies only to critical situations where responsible disclosure procedures would not save funds due to the urgency of the exploit, and it is not intended for routine security testing or vulnerability reporting.

- Mandatory Return of Rescued Funds: Under the terms of the Safe Harbor, whitehats are required to return all rescued assets to a pre-designated recovery address controlled by the protocol within 72 hours of recovering them. This ensures that recovered funds are quickly secured, preventing delay or potential loss.

- Clear Guidelines and Legal Protection: The agreement establishes strict rules for how whitehats must operate during an exploit, ensuring recovery efforts are conducted professionally and safely, minimizing the risk of mistakes or further damage to the protocol. By adhering to these guidelines, whitehats can limit their potential legal exposure, allowing them to act in good faith without fear of liability.

- Incentivized Rescue Efforts: To motivate whitehats to act during critical situations, the agreement offers a bounty system similar to a bug bounty. Whitehats are rewarded with a percentage of the recovered assets, up to a predefined cap, for their successful interventions.

For more information, check out the Safe Harbor Agreement here.

Rationale

Uniswap, by design, does not include a pause function, meaning the protocol cannot be halted in the event of an exploit. This makes it essential to have a mechanism that allows rapid response and asset recovery during emergencies.

The Safe Harbor Agreement provides this necessary solution, empowering whitehats to act immediately during an exploit, offering a swift and structured recovery process without needing to pause the protocol.

Benefits of adopting the Safe Harbor Agreement include:

- Agile Defense Against Exploits: Whitehats are authorized to intervene as soon as an active exploit is detected, enabling them to respond faster than traditional methods. This ensures that Uniswap is protected against threats even without the ability to halt the protocol. Immediate action minimizes the window for malicious actors, reduces damages, and accelerates the recovery of assets during critical moments.

- Clarified Rescue Process: The agreement ensures that every step, from intervention to fund recovery, is predetermined and streamlined. Whitehats know exactly where to send recovered funds, preventing chaotic negotiations or rushed decisions during an exploit. This clarity ensures efficient, decisive action when it matters most.

- Clear Financial Boundaries: The predefined bounty system, with a cap matching Uniswap Labs' existing bug bounty for V3, ensures that whitehats are incentivized fairly without creating conflicting priorities between exploit intervention and standard vulnerability disclosure. By setting expectations upfront, it eliminates post-exploit negotiations, ensuring funds are returned promptly without attempts to change the reward amount, keeping the process fair and transparent.

- Aligning with Industry Best Practices: By adopting the Safe Harbor Agreement, Uniswap aligns itself with leading security practices across the industry, reinforcing its commitment to staying at the forefront of protocol security.

Adoption of the agreement complements audits by providing an additional layer of security, ensuring that the protocol is better prepared to respond to active threats.

Adoption Details

Uniswap will adopt the agreement with the following parameters. For a full description of these adoption details, review the Safe Harbor for Protocols document.

1. Asset Recovery Address: Addresses controlled by Uniswap, which recovered funds will be returned to in the event of a hack. Source

Chain

Address

Ethereum

0x1a9C8182C09F50C8318d769245beA52c32BE35BC

Arbitrum

0x2BAD8182C09F50c8318d769245beA52C32Be46CD

Avalanche

0xeb0BCF27D1Fb4b25e708fBB815c421Aeb51eA9fc

Base

0x31FAfd4889FA1269F7a13A66eE0fB458f27D72A9

Blast

0x2339C0d23b60739B3E5ABF201F05903D24A26C77

Boba

0x53163235746CeB81Da32293bb0932e1A599256B4

BSC

0x341c1511141022cf8eE20824Ae0fFA3491F1302b

Celo

0x0Eb863541278308c3A64F8E908BC646e27BFD071

Filecoin EVM

0xFf3b2DA1379cc67cc2755194604713f10b820b0E

Gnosis

0xfFA5599136fBaB9af7799A6703b57BB33E5390Cf

Linea

0x581F86Da293A1D5Cd087a10E7227a75d2d2201A8

Manta Pacific

0x683553d74D9779955a15d57D208234C956B6Eae6

Mantle

0x9b7aC6735b23578E81260acD34E3668D0cc6000A

Moonbeam

0xB2af16D6c7074228fC487F17929De830303E6531

Optimism

0xa1dD330d602c32622AA270Ea73d078B803Cb3518

Polygon

0x8a1B966aC46F42275860f905dbC75EfBfDC12374

Polygon zkEVM

0x1808cc3ffb04e8bB67BfEB5510D44e62cF380717

Redstone

0x2d00e94d78Fc307FC5E6195BBe2fB6aFC2FC07d4

Rootstock

0x38aE7De6f9c51e17f49cF5730DD5F2d29fa20758

Scroll

0xEfc9D1096fb65c832207E5e7F13C2D1102244dbe

Sei

0xe75358526ef4441db03ccaeb9a87f180fae80eb9

Taiko

0xf6b53E8dA8bc7dbddB8E7B39635d17D7CCdCD6E5

WorldChain

0xcb2436774C3e191c85056d248EF4260ce5f27A9D

ZkSync

0x2BAD8182C09F50c8318d769245beA52C32Be46CD

Zora

0x36eEC182D0B24Df3DC23115D64DB521A93D5154f

1. Scope: List of all on-chain assets protected under Safe Harbor.[V1 Source](), [V2 Source 1](), [V2 Source 2](), [V3 Source](), [UniStaker and V3FactoryOwner Source](), [Franchiser Factory Source]()

Chain

Name

Address

Type (None, Existing Only, All)

Ethereum

UniswapV1Factory

0xc0a47dFe034B400B47bDaD5FecDa2621de6c4d95

All

Ethereum

UniswapV2Factory

0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f

All

Arbitrum

UniswapV2Factory

0xf1D7CC64Fb4452F05c498126312eBE29f30Fbcf9

All

Avalanche

UniswapV2Factory

0x9e5A52f57b3038F1B8EeE45F28b3C1967e22799C

All

Base

UniswapV2Factory

0x8909Dc15e40173Ff4699343b6eB8132c65e18eC6

All

Blast

UniswapV2Factory

0x5C346464d33F90bABaf70dB6388507CC889C1070

All

Boba

UniswapV2Factory

0x40a26d18440948d8eE121b78ca4e88C37D30143b

All

BSC

UniswapV2Factory

0x8909Dc15e40173Ff4699343b6eB8132c65e18eC6

All

Celo

UniswapV2Factory

0x114a43df6c5f54ebb8a9d70cd1951d3dd68004c7

All

Filecoin EVM

UniswapV2Factory

0x114a43df6c5f54ebb8a9d70cd1951d3dd68004c7

All

Gnosis

UniswapV2Factory

0x8c8b524ce7c9D2e3f59aB6711bE4Ac826FA46a0f

All

Linea

UniswapV2Factory

0x114a43df6c5f54ebb8a9d70cd1951d3dd68004c7

All

Moonbeam

UniswapV2Factory

0x114a43df6c5f54ebb8a9d70cd1951d3dd68004c7

All

Optimism

UniswapV2Factory

0x0c3c1c532F1e39EdF36BE9Fe0bE1410313E074Bf

All

Polygon

UniswapV2Factory

0x9e5A52f57b3038F1B8EeE45F28b3C1967e22799C

All

Rootstock

UniswapV2Factory

0x114a43df6c5f54ebb8a9d70cd1951d3dd68004c7

All

Scroll

UniswapV2Factory

0x114a43df6c5f54ebb8a9d70cd1951d3dd68004c7

All

WorldChain

UniswapV2Factory

0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f

All

Zora

UniswapV2Factory

0x0F797dC7efaEA995bB916f268D919d0a1950eE3C

All

Ethereum

UniswapV3Factory

0x1F98431c8aD98523631AE4a59f267346ea31F984

All

Arbitrum

UniswapV3Factory

0x1F98431c8aD98523631AE4a59f267346ea31F984

All

Avalanche

UniswapV3Factory

0x740b1c1de25031C31FF4fC9A62f554A55cdC1baD

All

Base

UniswapV3Factory

0x33128a8fC17869897dcE68Ed026d694621f6FDfD

All

Blast

UniswapV3Factory

0x792edAdE80af5fC680d96a2eD80A44247D2Cf6Fd

All

Boba

UniswapV3Factory

0xFFCd7Aed9C627E82A765c3247d562239507f6f1B

All

BSC

UniswapV3Factory

0xdB1d10011AD0Ff90774D0C6Bb92e5C5c8b4461F7

All

Celo

UniswapV3Factory

0xAfE208a311B21f13EF87E33A90049fC17A7acDEc

All

Filecoin EVM

UniswapV3Factory

0xB4C47eD546Fc31E26470a186eC2C5F19eF09BA41

All

Gnosis

UniswapV3Factory

0xe32F7dD7e3f098D518ff19A22d5f028e076489B1

All

Linea

UniswapV3Factory

0x31FAfd4889FA1269F7a13A66eE0fB458f27D72A9

All

Manta Pacific

UniswapV3Factory

0x06D830e15081f65923674268121FF57Cc54e4e23

All

Mantle

UniswapV3Factory

0x0d922Fb1Bc191F64970ac40376643808b4B74Df9

All

Moonbeam

UniswapV3Factory

0x28f1158795A3585CaAA3cD6469CD65382b89BB70

All

Optimism

UniswapV3Factory

0x1F98431c8aD98523631AE4a59f267346ea31F984

All

Polygon

UniswapV3Factory

0x1F98431c8aD98523631AE4a59f267346ea31F984

All

Polygon zkEVM

UniswapV3Factory

0xff83c3c800Fec21de45C5Ec30B69ddd5Ee60DFC2

All

Redstone

UniswapV3Factory

0xece75613Aa9b1680f0421E5B2eF376DF68aa83Bb

All

Rootstock

UniswapV3Factory

0xaF37EC98A00FD63689CF3060BF3B6784E00caD82

All

Scroll

UniswapV3Factory

0x70C62C8b8e801124A4Aa81ce07b637A3e83cb919

All

Sei

UniswapV3Factory

0x75FC67473A91335B5b8F8821277262a13B38c9b3

All

Taiko

UniswapV3Factory

0x75FC67473A91335B5b8F8821277262a13B38c9b3

All

WorldChain

UniswapV3Factory

0x7a5028BDa40e7B173C278C5342087826455ea25a

All

ZkSync

UniswapV3Factory

0x8FdA5a7a8dCA67BBcDd10F02Fa0649A937215422

All

Zora

UniswapV3Factory

0x7145F8aeef1f6510E92164038E1B6F8cB2c42Cbb

All

Ethereum

FranchiserFactory

0xf754A7E347F81cFdc70AF9FbCCe9Df3D826360FA

All

Ethereum

UniStaker

0xE3071e87a7E6dD19A911Dbf1127BA9dD67Aa6fc8

All

Ethereum

V3FactoryOwner

0x2e27332b25Ce245F6628377bc83573A001313C58

All

- "All": The Safe Harbor Agreement will cover both the subcontracts currently deployed under this contract and any future subcontracts deployed through it. This ensures that all present and future subcontracts are protected.

- Contact Details: Designated security contact for Uniswap

- Name: Erin Koen

- Contact Information: erin@uniswapfoundation.org

- Every 4 months. The person of contact will create a post to state their availability and whether or not they can continue being the person of contact.

- Every 4 months. The person of contact will create a post to state their availability and whether or not they can continue being the person of contact.

- Name: Erin Koen

- Contact Information: erin@uniswapfoundation.org

- Every 4 months. The person of contact will create a post to state their availability and whether or not they can continue being the person of contact.

- Bounty Terms: Predetermined rewards for successful whitehats that protect protocol funds

- Bounty Percentage: 10% of recovered funds.

- Bounty Cap (USD): $2.25m

- For clarification, the bounty is per whitehat per hack event. Please see the legal document for additional clarification.

- Retainable: True

- This means that whitehats are allowed to retain their bounty directly from the recovered assets. After rescuing funds during an exploit, whitehats may deduct their bounty from the total recovered amount before transferring the remainder to the protocol's designated asset recovery address. This streamlines the payout process, ensuring whitehats are rewarded promptly while still adhering to predefined bounty terms.

- Identity Verification: Anonymous

- Whitehats are allowed to remain anonymous and are not required to provide their legal name or undergo identity verification. This ensures privacy for whitehats while still enabling them to participate in the bounty program and assist during exploits without revealing personal information.

- Diligence Requirements: None

- Bounty Percentage: 10% of recovered funds.

- Bounty Cap (USD): $2.25m

- For clarification, the bounty is per whitehat per hack event. Please see the legal document for additional clarification.

- Retainable: True

- This means that whitehats are allowed to retain their bounty directly from the recovered assets. After rescuing funds during an exploit, whitehats may deduct their bounty from the total recovered amount before transferring the remainder to the protocol's designated asset recovery address. This streamlines the payout process, ensuring whitehats are rewarded promptly while still adhering to predefined bounty terms.

- Identity Verification: Anonymous

- Whitehats are allowed to remain anonymous and are not required to provide their legal name or undergo identity verification. This ensures privacy for whitehats while still enabling them to participate in the bounty program and assist during exploits without revealing personal information.

- Diligence Requirements: None

Implementation Plan

1. Register Agreement On-Chain:

2. The agreement will be registered on Ethereum in the Safe Harbor Registry at address 0x8f72fcf695523a6fc7dd97eafdd7a083c386b7b6, including all adoptionDetails. This ensures transparency and immutability.

3. The agreement will be registered on Ethereum in the Safe Harbor Registry at address 0x8f72fcf695523a6fc7dd97eafdd7a083c386b7b6, including all adoptionDetails. This ensures transparency and immutability.

4. Communicate Adoption:

5. An official announcement will be made across all Uniswap communication channels, explaining the adoption and its significance to the community.

6. An official announcement will be made across all Uniswap communication channels, explaining the adoption and its significance to the community.

7. Future Updates to Scope:

8. New versions of Uniswap (e.g., V4) will be reviewed and added to the Safe Harbor Agreement scope via Uniswap Governance vote, ensuring continued protection for all new contracts and functionalities.

9. New versions of Uniswap (e.g., V4) will be reviewed and added to the Safe Harbor Agreement scope via Uniswap Governance vote, ensuring continued protection for all new contracts and functionalities.

Conclusion

Adopting the SEAL Whitehat Safe Harbor Agreement equips Uniswap with a rapid response mechanism for active exploits, enabling whitehats to step in effectively when needed most. The agreement provides clear guidelines for action, increasing the protection of user funds and demonstrating Uniswap's commitment to proactive security.

References

- SEAL Whitehat Safe Harbor Agreement: GitHub Repository

- SEAL Whitehat Safe Harbor Agreement Overview: Notion

- Uniswap Bug Bounty: Uniswap Labs Bug Bounty Update

Please share your thoughts and feedback in the discussion below before the proposal moves to a formal vote.