Article Information

Authors: Michael Bacina, Steven Pettigrove, Jake Huang
Service: Blockchain
Sector: Financial Services, FinTech, IT & Telecommunications

Security Alliance proposes Whitehat Safe Harbor to secure Web3

Michael Bacina, Steven Pettigrove and Jake Huang of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

A leading group of Web3 security researchers and lawyers have launched a request for comment on the Whitehat Safe Harbor Agreement, a new security approach to assist in reducing blockchain hacks. Piper Alderman was pleased to collaborate with the Security Alliance (SEAL), Gabriel Shapiro, the Lexpunk coalition, Debevoise & Plimpton LPP, and the policy teams at Paradigm and A16Z Crypto, among many others, on this ground-breaking project.

A leading group of Web3 security researchers and lawyers have launched a request for comment on a new security approach to assist in reducing blockchain hacks. The Whitehat Safe Harbor Agreement is intended to incentivize "Whitehats", ethical security hackers, to rescue at-risk crypto assets where an active blockchain exploit is underway. The initiative is led by the Security Alliance (**SEAL**), a non-profit founded by leading security researcher samczsun and backed by a broad and international industry coalition with a view to addressing some of the key security challenges in the space.

Hacks and exploits have been a core concern in the growth of Web3 technologies. In 2022, nearly USD$650 million in assets was stolen in the Ronin bridge hack alone. An attack on the Nomad bridge later that year netted nearly USD $200 million in stolen funds. Early members of the Security Alliance were involved in identifying the root cause of the hack and helping the Nomad project recover USD $38.8 million in funds from several whitehats who had intentionally drained the bridge to protect funds from the attackers. Crypto bridges are software protocols that enable communication and interaction between different blockchains and effectively enable value to be transferred across blockchains.

The Safe Harbor initiative is a pre-emptive security measure for protocols, similar to a bug bounty. It is a framework specifically for *active exploits*, i.e. situations where a vulnerability has begun to be exploited by a malicious actor. If a protocol has adopted the Whitehat Safe Harbor Agreement before such an incident occurs, whitehats will have clarity on how to act in a potential rescue, and will be more likely to help intervene.

A blockchain protocol can adopt the Whitehat Safe Habor Agreement through a governance vote of tokenholders or alternative decision making process. The protocol would need to first identify:

- Which assets are in-scope for the agreement (e.g. any ERC20 token at a specific address)?
- What reward will be given to successful whitehat rescues (e.g. 10% of rescued funds capped at USD$1m)?
- Where should rescued funds be returned (e.g. a specific multisig or treasury address)?

If adopted, the Whitehat Safe Harbor Agreement forms part of the website's terms of service to enable users of the protocol to pre-emptively agree to whitehat rescues in the event of an exploit. This agreement is intended to incentivize whitehat hackers to rescue funds by offering agreed rewards and pre-emptive legal releases from the protocol and its users, and reducing the risk of criminal prosecution. The whitehat must comply with the procedures in the agreement and return funds to a designated asset recovery address in order to benefit from the protections under the safe harbor.

The Security Alliance, or SEAL, is the coalition behind the SEAL drills initiative, which allows developer teams to war-game security incident scenarios, and the SEAL 911 Emergency Hotline, which enables users, developers and security researches who need access to urgent security advice, help with disclosing a critical vulnerability, or to simply sync on progress with other researchers to connect with a team of carefully vetted expert volunteers. Over the past 6 months, SEAL 911 has helped disrupt, intercept, and remediate several hacks, as well as assisted numerous people with other security problems.

The request for comment runs until 14 March 2024. The proposal is the result of more than 18 months of work. Piper Alderman was pleased to collaborate on the Whitehat Safe Harbor Agreement alongside the Security Alliance and leading blockchain and cyber security lawyers including Gabriel Shapiro, the Lexpunk coalition, Debevoise & Plimpton LPP, and the policy teams at Paradigm and A16Z Crypto, among many others.