EverETH

EverETH Responsible Disclosure Policy

At EverETH, we take the security of our products and services very seriously. We appreciate the efforts of security researchers and the wider cybersecurity community in identifying and responsibly disclosing potential vulnerabilities.

This Responsible Disclosure Policy outlines the guidelines and processes for reporting potential security vulnerabilities to EverETH. By following these guidelines, researchers can help us improve the security of our systems and protect our users' data and assets.

Scope

This policy applies to all EverETH products, services, websites, and infrastructure, including but not limited to:

- EverETH.net and associated websites
- EverETH Reflect protocol and smart contracts
- EETH token and related smart contracts
- EverETH dApps and decentralised applications
- EverETH backend systems and APIs

Guidelines for Researchers

1. **Authorised Testing**: Security research and testing should be conducted only on systems and assets owned or operated by EverETH. Any attempts to access or test systems outside the scope of this policy may be considered unauthorized and potentially unlawful.

2. **Safe Harbor**: EverETH will not initiate or recommend legal action against researchers who follow this policy's guidelines and act in good faith to disclose potential vulnerabilities responsibly.

3. **Vulnerability Reporting**: If you discover a potential security vulnerability, please report it to us immediately by sending an email to [security@evereth.net]. Please

include detailed information about the vulnerability, steps to reproduce it, and any relevant technical details or proof of concept.

4. **Confidentiality**: EverETH requests that researchers do not disclose or discuss the potential vulnerability publicly until it has been addressed and mitigated by our team. This helps us protect our users and ecosystem from potential harm.

5. **Cooperation**: We encourage researchers to cooperate with our security team during the vulnerability disclosure process. This may involve providing additional information, clarification, or assistance as needed.

6. **Responsible Disclosure**: EverETH expects researchers to act responsibly and ethically when disclosing vulnerabilities. Researchers should not engage in any activities that could cause harm, disrupt our services, or violate the privacy of our users.

EverETH's Commitments

1. **Acknowledgment**: EverETH will acknowledge receipt of vulnerability reports within 72 hours and provide regular updates on the status of the investigation and remediation efforts.

2. **Timely Resolution**: We will make every effort to address and mitigate confirmed vulnerabilities in a timely manner, prioritising critical issues that pose a significant risk to our users or systems.

3. **Coordination**: EverETH will coordinate the disclosure and release of vulnerability details with the reporting researcher, ensuring that appropriate remediation measures are in place before public disclosure.

4. **Recognition**: EverETH recognizes and appreciates the efforts of security researchers who responsibly disclose vulnerabilities. We may publicly acknowledge researchers' contributions, subject to their consent and preferences.

5. **Bug Bounty Program**: EverETH may consider implementing a bug bounty program in the future to further incentivize and reward security research efforts.

By adhering to this Responsible Disclosure Policy, security researchers and EverETH can work together to enhance the security of our products, services, and infrastructure, ultimately protecting our users and the wider cryptocurrency and DeFi ecosystem.

If you have any questions or concerns about this policy, please contact us at [support@evereth.net].

@EverETHofficial

@EverETHofficial