## 范围

2023.6.26之前所有Final的ERC提案

## 分类

(1)Token (2) Address (3) ENS (4) Interface (5)Owner (6)Package (7)Sign (8) Wallet (9)Protocol (10)NFT (11)Proxy (12)Loan (13)Vault

## 共同问题

（1）缺少最佳实践方案 （2）缺少编码规范（3）缺少安全规范 （4）缺少使用指南

## 问题分类

### Token

涉及提案: （1）ERC20-Token Standard（2）ERC777-Token Standard（3）ERC1155-Multi Token Standard（4）ERC1363-Payable Token（5）ERC2612-Permit Extension for EIP-20 Signed Approvals（6）ERC5507-Refundable Tokens（7）ERC5528-Refundable Fungible Token（8）ERC5679-Token Minting and Burning

存在问题:

Multiple withdrawal

1. ERC20-[IEEE S&P Workshop Resolving the Multiple Withdrawal Attack on ERC20 Tokens](https://www.pulpspy.com/papers/2019_sb_erc20.pdf)

Arithmetic Over/Under Flows.

1. ERC20-[BEC token](https://etherscan.io/address/0xc5d105e63711398af9bbff092d4b6769c82f793d)

Re-entrancy

1. ERC20-[DAO](https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/)
2. ERC777-[uniswap](https://paper.seebug.org/1182/)

Unchecked return values

1. [eth transfer](https://medium.com/daox/three-methods-to-transfer-funds-in-ethereum-by-means-of-solidity-5719944ed6e9)

Frozen Ether

1. token-[parity wallet](https://www.parity.io/blog/security-alert-2/)

Unprotected Ether Withdrawal

1. token-[rubixi](https://etherscan.io/address/0xe82719202e5965Cf5D9B6673B7503a3b92DE20be#code)

State variable manipulation

1. [parity](https://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/)

Balance manipulation

1. token-[selftdestruct](http://danielszego.blogspot.com/2018/03/solidity-security-patterns-forcing.html)

Access control

1. ERC20-[parity](http://parity)
2. ERC777-[finishMinting()](https://verasity.io/documents/smart_contract_audit.pdf)

Unclear compiler version

1. ERC20/777/2612/5679 EIP中未标注版本要求

参考:

1. [tokenhook: Secure ERC-20 smart contract](https://arxiv.org/pdf/2107.02997v1.pdf)
2. CMAI2023-[The Analysis of the Risks and Improvements of ERC20 Tokens](https://drpress.org/ojs/index.php/HSET/article/view/6713/6508)
3. iosiro [Verasity ERC-777 Token](https://verasity.io/documents/smart_contract_audit.pdf)
4. consensys [ERC1155Proxy Audit](https://github.com/ConsenSys/0x-audit-report-2019-05)
5. Security Considerations：ERC1363、ERC2612、ERC5507、ERC5528、ERC5679

### Address

涉及提案：（1）ERC55-Mixed-case checksum address encoding（2）ERC1271-Standard Signature Validation Method for Contracts（3）ERC2098-Compact Signature Representation

存在问题:

code security

gas security

Arithmetic Over/Under Flows.

参考:

1. Security Considerations：ERC1271

### ENS

涉及提案: (1) ERC137-Ethereum Domain Name Service - Specification (2)ERC162-Initial ENS Hash Registrar (3)ERC181-ENS support for reverse resolution of Ethereum addresses(4) ERC4834-Hierarchical Domains

存在问题:

domain security

privilege issue

code security

logical security

Arithmetic Over/Under Flows.

参考:

1. [Consensys ens audit report 2019-02](https://github.com/ConsenSys/ens-audit-report-2019-02)
2. [ENS register](https://gist.github.com/maurelian/f96c2a6b9b13ae9e351a6695321b350b)
3. Security Considerations：ERC4834

### Interface

涉及提案: (1) ERC165-Standard Interface Detection (2)ERC820-Pseudo-introspection Registry Contract (3) ERC1046-tokenURI Interoperability (4) ERC1820-Pseudo-introspection Registry Contract(5) ERC3668-CCIP Read: Secure offchain data retrieval (6)ERC5219-Contract Resource Requests (7) ERC5646-Token State Fingerprint (8)ERC5732-Commit Interface (9)ERC5750-General Extensibility for Method Behaviors

存在问题:

lack of security standards

lack of code standards

SSRF

replay

front-run

crypto

参考:

1. Security Considerations：ERC820、ERC1046、ERC3668、ERC5219、ERC5646、ERC5732、ERC5750
2. Optimism Smart Contracts Audit - [ERC1820 part](https://blog.openzeppelin.com/optimism-smart-contracts-audit)

### Owner

涉及提案：（1）ERC173-Contract Ownership Standard（2）ERC5313-Light Contract Ownership

存在问题：

privilege issue

Unclear compiler version

参考:

1. Security Considerations: ERC173、ERC5313

### Package

涉及提案: (1)ERC190-Ethereum Smart Contract Packaging Standard(2) ERC2678-Revised Ethereum Smart Contract Packaging Standard (EthPM v3)

存在问题:

lack of security standards

参考:

1. Security Considerations: ERC2678

### Sign

涉及提案: （1）ERC191-Signed Data Standard

存在问题:

code security

replay

lack of ecrecover check

Phishing for signatures

参考:

1. [Monethic signature](https://medium.com/coinmonks/ethereum-signatures-for-hackers-and-auditors-101-4da766cd6344)

### Wallet

涉及提案: (1)ERC600-Ethereum purpose allocation for Deterministic Wallet(2) ERC601-Ethereum hierarchy for deterministic wallets

存在问题:

lack of security standards

lack of code standards

参考:

1. github: [Standardizing of HD wallet derivation paths (BIP32, BIP39, BIP44) #84](https://github.com/ethereum/EIPs/issues/84)

### Protocol

涉及提案: (1) ERC681-URL Format for Transaction Requests (2)ERC4804-Web3 URL to EVM Call Message Translation

存在问题:

lack of security standards

lack of code standards

参考:

1. Security Considerations: ERC481

### NFT

涉及提案:(1)ERC721-Non-Fungible Token Standard (2)ERC2309-ERC-721 Consecutive Transfer Extension (3)ERC2981-NFT Royalty Standard (4)ERC3475-Abstract Storage Bonds (5) ERC3525-Semi-Fungible Token

(6)ERC4400-EIP-721 Consumable Extension(7)ERC4519-Non-Fungible Tokens Tied to Physical Assets(8)ERC4906-EIP-721 Metadata Update Extension(9)ERC4907-Rental NFT, an Extension of EIP-721 (10)ERC4955-Vendor Metadata Extension for NFTs(11)ERC5006-Rental NFT, NFT User Extension(12)ERC5007-Time NFT, ERC-721 Time Extension (13)ERC5023-Shareable Non-Fungible Token (14)ERC5169-Client Script URI for Token Contracts (15)ERC5192-Minimal Soulbound NFTs (16)ERC5267-Retrieval of EIP-712 domain (17)ERC5375-NFT Author Information and Consent (18) ERC5380-ERC-721 Entitlement Extension (19) ERC5484-Consensual Soulbound Tokens (20)ERC5489-NFT Hyperlink Extension (21)ERC5507-Refundable Tokens

(22)ERC5570-Digital Receipt Non-Fungible Tokens (23)ERC5606-Multiverse NFTs (24)ERC5615-ERC-1155 Supply Extension (25)ERC5773-Context-Dependent Multi-Asset Tokens (26)ERC6059-Parent-Governed Nestable Non-Fungible Tokens

(27)ERC6105-No Intermediary NFT Trading Protocol (28)ERC6147-Guard of NFT/SBT, an Extension of ERC-721 (29)ERC6150-Hierarchical NFTs (30) ERC6220-Composable NFTs utilizing Equippable Parts (31)ERC6454-Minimal Transferable NFT detection interface (32)ERC6672-Multi-redeemable NFTs

存在问题：

Arithmetic Over/Under Flows.

1. ERC2309-[opensea standards](https://github.com/OpenZeppelin/openzeppelin-contracts/issues/2355#issuecomment-1200144796)
2. ERC721-OMNI Real Estate Exploit

Reentrancy

1. ERC721-n00dleswap

DDOS

1. ERC721-LooksRare

Access control

1. ERC721-Sevens

privilege issue

logic issue

crypto security

iot security

off-chain data security

SSRF

front-run

参考:

1. ERC5192、ERC5489-[bgin study report](https://bgin-global.org/pdf/BGIN_WD_SR008_Soulbound_Tokens_(SBTs)_Part_1.pdf)
2. [Hacken NFT audit](https://hacken.io/discover/security-audit-for-nft-guide-for-founders-and-managers/)
3. github-[ERC2309](https://github.com/OpenZeppelin/openzeppelin-contracts/issues/3711)
4. solidify [Yieldification ERC2981 part](https://solidity.finance/audits/Yieldification/)
5. Security Considerations: ERC3475、ERC4400、ERC4519、ERC4906、ERC4955、ERC5169、ERC5267、ERC5375、ERC5570、ERC5615、ERC5773、ERC6059、ERC6105、ERC6147、ERC6220、ERC6454、ERC6672
6. salus [ERC3525](https://apiv1.salusec.io/api/v1/salus/contract/certificate/full/ERC3525_audit_report_2023-03-10.pdf)
7. solidify [Netvrk ERC4907](https://solidity.finance/audits/Netvrk/)

### Proxy

涉及提案： （1）ERC1167-Minimal Proxy Contract（2）ERC1967-Proxy Storage Slots（3）ERC2535-Diamonds, Multi-Facet Proxy（4）ERC3448-MetaProxy Standard

存在问题:

lack of usage standards

slot security

privilege issue

参考:

1. OPENZEPPELIN [Compound III Audit ERC1967 part](https://blog.openzeppelin.com/compound-iii-audit)
2. Security Considerations: ERC2535

### Loan

涉及提案：ERC3156-Flash Loans

存在问题:

callback security

Multiple withdrawal

interest rate attack

Arithmetic Over/Under Flows.

Treasury draining

DOS

参考:

1. Security Considerations: ERC3156
2. OPENZEPPELIN-[Neptune Mutual Audit ERC3156 part](https://blog.openzeppelin.com/neptune-mutual-audit)

### Vault

涉及提案:ERC4626-Tokenized Vaults

存在问题:

front-run

Unsafe ABI encoding

Arithmetic Over/Under Flows.

Unclear compiler version

Access control

Unchecked return values

参考:

1. openzeppelin [2022-10-ERC4626](https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/audits/2022-10-ERC4626.pdf)

### 其他

ERC137-CVE-2020-5232

OPENZEPPELIN EIP-4337 – [Ethereum Account Abstraction Audit](https://blog.openzeppelin.com/eth-foundation-account-abstraction-audit)

hacken [ERC3643](https://tokeny.com/wp-content/uploads/2023/04/Tokeny_TREX-v4_SC_Audit_Report.pdf)

## 安全建议

（1）最佳实践方案 （2）编码规范（3）安全规范 （4）使用指南

分类:

token:

会议记录：

主要问题：函数规范，功能限制

eip的生态比较野蛮

大家没有很好的关注eip的完成度，eip协议应该有一定的要求，会影响以太坊的生态，会造成安全问题，规范也会对撰写者有一定筛选，对书写者要有一定要求；

讨论：

（后续工作）是否要规范函数的定义方法，支持类型，书写格式，安全结构的基础上，对eip进行进一步的定义，不能太开放式