EOSIO.WPS

智能合约安全审计报告

2020-04-15

1. 概要

在本报告中，我们对 EOSIO.WPS 项目的智能合约代码进行安全审计。我们的任务是发现和指出项目里智能合约代码中的安全问题。

2. 声明

慢雾仅就本报告出具前已经发生或存在的事实出具本报告，并就此承担相应责任。对于出具以后发生或存在的事实，慢雾无法判断其智能合约安全状况，亦不对此承担责任。本报告所作的安全审计分析及其他内容，仅基于信息提供者截至本报告出具时向慢雾提供的文件和资料(简称“已提供资料”)。慢雾假设：已提供资料不存在缺失、被篡改、删减或隐瞒的情形。如已提供资料信息缺失、被篡改、删减、隐瞒或反映的情况与实际情况不符的，慢雾对由此而导致的损失和不利影响不承担任何责任。

3. 总结

在本报告中，我们对 EOSIO.WPS 项目的智能合约代码进行安全审计。审计没有发现严重、高危的问题，发现了一些**中危、低危程度的安全问题。**经双方沟通反馈，问题均已修复。

4. 项目概述

4.1 项目描述

我们审计了 EOSIO.WPS 的智能合约代码，如下是相关的文件信息:

项目合约地址：https://github.com/EOS-Nation/eos-wps

审计初始 commit：51399034ca947c66cc6c4429bd439f41308f5340

最终修复 commit：e115197eb78b6f6a851f253f68784324383fae14

4.2 项目结构

```
./src
├── activate.cpp
├── claims.cpp
├── comments.cpp
├── complete.cpp
├── deposits.cpp
├── drafts.cpp
├── eosio.wps.cpp
├── on_notify.cpp
├── proposers.cpp
├── refresh.cpp
├── settings.cpp
├── utils
│   └── get_tx_id.cpp
└── vote.cpp

./external
├── eosio.system
│   ├── eosio.system.abi
│   ├── eosio.system.wasm
│   └── include
│       └── eosio.system
└── eosio.token
```

```
├── eosio.token.abi
├── eosio.token.wasm
├── include
│   └── eosio.token
└── src
    └── eosio.token.cpp

./include
└── eosio.wps
    └── eosio.wps.hpp
```

4.3 合约架构

EOSIO.WPS 主要分成四个部分：drafts、 proposals 、vote 和 complete，主要逻辑分别位于 drafts.cpp、activate.cpp、vote.cpp 和 complete.cpp 中。用户需要首先通过 drafts.cpp 中的 `submitdraft()` 函数提交提案，然后发送 100 EOS 到 合约中并通过 activate.cpp 中的 `activate()` 函数激活提案进入投票流程。每一个投票周期结束后，任意用户可手动调用 complete.cpp 中的 `complete()` 函数进行结算，领取提案预算。

5. 审计方法

我们的智能合约安全审计流程包含两个步骤:

- 使用开源或内部自动化分析的工具对合约代码中常见的安全漏洞进行扫描和测试。
- 人工审计代码的安全问题，通过人工分析合约代码，查找代码中潜在的安全问题。

如下是合约代码审计过程中我们会重点审查的常见漏洞列表:

- 溢出审计
- 权限控制审计
- 权限过大审计
- 硬编码地址安全
- 显现编码安全
- 异常校验审计
- 类型安全审计
- 性能优化审计
- 设计逻辑审计
- 拒绝服务审计
- 回滚攻击审计
- 重放攻击审计
- 假通知审计
- 假错误通知审计

- 假币审计
- 随机数安全审计
- 粉尘攻击安全审计
- 微分叉安全审计
- 排挤攻击安全审计

6 审计结果

6.1 严重漏洞

严重漏洞会对智能合约的安全造成重大影响，强烈建议修复严重漏洞。

经过审计该项目未发现严重漏洞。

6.2 高危漏洞

高危漏洞会影响智能合约的正常运行，强烈建议修复高危漏洞。

经过审计该项目未发现高危漏洞。

6.3 中危漏洞

中危漏洞会影响智能合约的运行，建议修复中危漏洞。

6.3.1 校验缺失

(1) setting.cpp 中的 `init()` 函数没有检查 `voting_interval` 是否大于一个月，如果 `voting_interval` 小于一个月，比方说 20 分钟，一个`duration` 为 5 的提案会在 5 个投票周期内拿完所有的预算，而不是 5 个月。

```
[[eosio::action]]
```

```
void wps::init( const wps_parameters params )
{
    require_auth( get_self() );
    const name ram_payer = get_self();

    check( !_state.exists(), "already initialized" );

    // define `settings`
    auto settings = params;

    //SlowMist// 未校验 voting_internal 值

    _settings.set( settings, ram_payer );

    // set available EOS as `available_funding`
    auto state = _state.get_or_default();
    state.available_funding = token::get_balance( CORE_TOKEN_CONTRACT, get_self(), CORE_SYMBOL.code() );

    // start of voting period will start at the nearest 00:00UTC
    const uint64_t now = current_time_point().sec_since_epoch();
    const time_point_sec current_voting_period = time_point_sec(now - now % DAY);

    // define `state`
    state.current_voting_period = current_voting_period;
    state.next_voting_period = state.current_voting_period + settings.voting_interval;
    _state.set( state, ram_payer );

    // check if WPS account has enough funding to initialize the first voting period
    check_available_funding();
}
```

修复情况：在 commit adc43133f2269b7f73e00b7fd26313a3c6a187d0 中修复。

6.3.2 逻辑缺陷

（1）complete.cpp 中 `copy_current_to_next_periods()` 函数同时复制了 `active` 和 `expired` 的提案到下一个周期，导致投票周期内出现过期提案。应只复制 `active` 提案到下一个周期。

```
void wps::copy_current_to_next_periods()
{
    const name ram_payer = get_self();
    auto state = _state.get();
```

```
    auto settings = _settings.get();

    // must calculate next_voting_period in case the next period has been changed caused by delayed complete action
    // cannot use `state.next_voting_period`
    const time_point_sec next_voting_period = current_time_point() + time_point_sec( settings.voting_interval );

    // lookup iterators
    auto current_periods_itr = _periods.find( state.current_voting_period.sec_since_epoch() );
    auto next_periods_itr = _periods.find( next_voting_period.sec_since_epoch() );

    // create new set of proposals
    if ( next_periods_itr == _periods.end() ) {
        _periods.emplace( ram_payer, [&]( auto& row ) {
            row.voting_period     = next_voting_period;

            //Slowmist// 复制了所有的提案，包含过期提案

            row.proposals         = current_periods_itr->proposals;
        });
    // insert proposal to old ones
    } else {
        _periods.modify( next_periods_itr, ram_payer, [&]( auto& row ) {
            row.proposals = current_periods_itr->proposals;
        });
    }
}
```

修复情况：在 commit e115197eb78b6f6a851f253f68784324383fae14 中修复。

（2）complete.cpp 文件中 `set_pending_to_active()` 函数每次只更新一个 `pending` 状态的提案，如果 `pending` 状态的提案多于一个，剩余的提案将不会被更新。

```
void wps::set_pending_to_active()
{
    auto index = _proposals.get_index<"bystatus"_n>();
    auto itr = index.find("pending"_n.value);

    if (itr == index.end()) return;

    index.modify( itr, same_payer, [&]( auto& row ) {
        row.status = "active"_n;
```

```
    });
}
```

修复情况：在 commit adc43133f2269b7f73e00b7fd26313a3c6a187d0 中修复。

（3）在 complete.cpp，第 29-32 行，由于当前的提案在更新投票周期前被复制到下一个周期，导致同一周期的 `pending` 提案和 `active` 提案被放置在不同的投票周期中。

```
[[eosio::action]]
void wps::complete( )
{
    // no authorization required (can be executed by any account)

    // is contract paused or not
    check_contract_active();

    // check if current voting period is completed
    check( is_voting_period_complete(), "[current_voting_period] is not completed");

    // check if account has enough funding
    check_available_funding();

    // update `votes` from eligible voters
    // any existing votes with voters with less than 100 EOS vpay will be removed
    refresh_proposals();

    // update `proposals::eligible` field for all active proposals
    update_eligible_proposals();

    // payouts of active proposals
    handle_payouts();

    // copy current proposals to next period
    copy_current_to_next_periods();

    // update current & next voting period
    update_to_next_voting_period();

    // set pending proposals to active status
    set_pending_to_active();
```

```
}
```

修复情况：在 commit e115197eb78b6f6a851f253f68784324383fae14 中修复。

6.4 低危漏洞

低危漏洞可能会影响未来版本代码中智能合约的操作，建议项目方自行评估和考虑这些问题是否需要修复。

6.4.1、校验缺失

(1) 提案发起人在提交提案的时候不需要先通过 proposer.cpp 提交发起人信息。

```
[[eosio::action]]
void wps::submitdraft(const name proposer,
                      const name proposal_name,
                      const string title,
                      const asset monthly_budget,
                      const uint8_t duration,
                      const map<name, string> proposal_json )
{
    require_auth( proposer );
    const name ram_payer = proposer;

    // get scoped draft
    drafts_table _drafts( get_self(), proposer.value );
    auto drafts_itr = _drafts.find( proposal_name.value );
    auto proposals_itr = _proposals.find( proposal_name.value );

    // check if proposer is eligible to activate proposal
    check_eligible_proposer( proposer );

    // validation
    check( proposals_itr == _proposals.end(), "[proposal_name] activated proposal already exists, try using a different proposal name" );
```

```
    check( drafts_itr == _drafts.end(), "[proposal_name] draft already exists, try using `modifydraft` or `canceldraft` or `modifybudget`" );
    check( proposal_name.length() > 2, "[proposal_name] should be at least 3 characters in length" );
    check( proposal_name.length() < 13, "[proposal_name] cannot exceed 12 characters in length" );
    check_title( title );
    check_monthly_budget( monthly_budget );
    check_duration( duration );

    //SlowMist// 无需先提交提案发起人信息

    // create draft proposal
    _drafts.emplace( ram_payer, [&]( auto& row ) {
        row.proposer            = proposer;
        row.proposal_name     = proposal_name;
        row.title               = title;
        row.monthly_budget    = monthly_budget;
        row.duration            = duration;
        row.total_budget      = asset{ monthly_budget.amount * duration, monthly_budget.symbol };
        row.proposal_json     = proposal_json;
    });

    create_deposit_account( proposer, ram_payer );
}
```

修复情况：经与项目方沟通后，确认此处问题忽略，强制要求申请人提交额外的信息是非必要的。

(2) 在 claim.cpp 文件第 17 行中，`proposer_itr` 在获取指针对应信息后才检查是否为 `end()`，应在定义后先检查是否为 `end()` 。

```
[[eosio::action]]
void wps::claim( const eosio::name proposal_name )
{
    // no authorization required (can be executed by any account)

    // static actions
    token::transfer_action transfer( CORE_TOKEN_CONTRACT, { get_self(), "active"_n });

    auto proposals_itr = _proposals.find( proposal_name.value );
    const eosio::name proposer = proposals_itr->proposer;
    const eosio::asset payouts = proposals_itr->payouts;
    const eosio::asset claimed = proposals_itr->claimed;
```

```
    // calculate claimable amount
    const eosio::asset claimable = payouts + claimed;

    check( proposals_itr != _proposals.end(), "[proposal_name] does not exist" );
    check( claimable.amount > 0, "no claimable amount" );

    transfer.send( get_self(), proposer, claimable, "wps::" + proposal_name.to_string() );

    add_claim( proposer, proposal_name, claimable );

    _proposals.modify( proposals_itr, same_payer, [&]( auto& row ) {
        row.claimed -= claimable;
    });
}
```

修复情况：在 commit f61a20fd9dc56be8d1cea5ff6d4d60bf421afdbb 中修复。

(3) 在 activate.cpp 文件中，`activate()` 函数有一个逻辑是检查提案在激活时是否在 `min_time_voting_end` 中。但是相同的逻辑没有体现在 complete.cpp 中的 `complete()` 函数中，该函数也存在激活提案的功能。

```
[[eosio::action]]
void wps::complete( )
{
    // no authorization required (can be executed by any account)

    // is contract paused or not
    check_contract_active();

    // check if current voting period is completed
    check( is_voting_period_complete(), "[current_voting_period] is not completed");

    // check if account has enough funding
    check_available_funding();

    // update `votes` from eligible voters
    // any existing votes with voters with less than 100 EOS vpay will be removed
    refresh_proposals();
```

```
    // update `proposals::eligible` field for all active proposals
    update_eligible_proposals();

    // payouts of active proposals
    handle_payouts();

    // set pending proposals to active status
    // SlowMist// 未校验提案必须在 min_time_voting_end 外
    set_pending_to_active();

    // update current & next voting period
    update_to_next_voting_period();

    // re-update `proposals::eligible`
    update_eligible_proposals();
}
```

修复情况：经与项目方沟通后，确认此问题忽略。检查 min_time_voting_end 的逻辑是为了防止用户在投票的最后几分钟激活提案而损失他的 EOS。

(4) 在 setting.cpp 文件中，`init()` 函数没有检查 `min_time_voting_end` 必须大于 `voting_interval`，且没有检查 `deposit_required` 和 `max_monthly_budget` 的 symbol 必须为 EOS。

```
[[eosio::action]]
void wps::init( const wps_parameters params )
{
    require_auth( get_self() );
    const name ram_payer = get_self();

    check( !_state.exists(), "already initialized" );

    // define `settings`
    auto settings = params;
    //Slowmist// 未对相关属性进行校验
```

```
    _settings.set( settings, ram_payer );

    // set available EOS as `available_funding`
    auto state = _state.get_or_default();
    state.available_funding = token::get_balance( CORE_TOKEN_CONTRACT, get_self(), CORE_SYMBOL.code() );

    // start of voting period will start at the nearest 00:00UTC
    const uint64_t now = current_time_point().sec_since_epoch();
    const time_point_sec current_voting_period = time_point_sec(now - now % DAY);

    // define `state`
    state.current_voting_period = current_voting_period;
    state.next_voting_period = state.current_voting_period + settings.voting_interval;
    _state.set( state, ram_payer );

    // check if WPS account has enough funding to initialize the first voting period
    check_available_funding();
}
```

修复情况：在 commit

0b41e951469ebed52d10e836b1e89bc40742664a,

1601d05cd01640da3bd1fbe046fe520913a3474b 中修复。

6.4.2 变量未使用

(1) 在 complete.cpp 文件第 57 行中，在 `handle_payouts()` 的 `claim` 变量未使用，可删除。

```
void wps::handle_payouts()
{
    // settings
    auto settings = _settings.get();
    auto state = _state.get();

    // static actions
    wps::claim_action claim( get_self(), { get_self(), "active"_n });

    // iterate proposals by active status
    for ( auto proposal_name : group_proposals( "active"_n ) ) {
        auto proposals_itr = _proposals.find( proposal_name.value );
```

```
        const eosio::asset monthly_budget = proposals_itr->monthly_budget;
```

修复情况：在 commit 031b72533a375c0aa22965debf2fcfa658567a7f 中修复。

(2) vote.cpp 文件第 87 行，`update_eligible_proposals` 函数中的 `proposer` 变量未使用。

```
void wps::update_eligible_proposals()
{
    // settings
    auto settings = _settings.get();
    auto state = _state.get();

    // containers
    eosio::asset total_payout = asset{ 0, symbol{ "EOS", 4 }};

    // filter out min voting threshold proposals
    std::map<int16_t, std::set<eosio::name>> proposals = sort_proposals_by_net_votes( "active"_n );

    // iterate proposals from highest to lowest net votes
    for ( auto itr = proposals.rbegin(); itr != proposals.rend(); ++itr ) {

        // iterate over proposals
        for ( auto proposal_name : itr->second ) {
            // proposal variables
            auto proposal_itr = _proposals.find( proposal_name.value );
            const int16_t total_net_votes = itr->first;
            const eosio::name proposer = proposal_itr->proposer;
            const eosio::asset monthly_budget = proposal_itr->monthly_budget;

            // min requirements for payouts
            const bool is_min_vote_margin = total_net_votes >= settings.vote_margin;
            const bool is_enough_budget = (total_payout + monthly_budget) <= settings.max_monthly_budget;

            // set eligible of proposal (true/false)
            _proposals.modify( proposal_itr, same_payer, [&]( auto& row ) {
                if ( is_enough_budget && is_min_vote_margin ) {
                    total_payout += monthly_budget;
                    row.eligible = true;
                } else {
                    row.eligible = false;
                }
```

```
            });
        }
    }
}
```

修复情况：在 commit 031b72533a375c0aa22965debf2fcfa658567a7f 中修复。

(3) vote.cpp 文件第 54 行 `proposals_itr` 变量未使用。

```
void wps::update_vote( const name voter, const name proposal_name, const name vote )
{
    // validate vote
    auto votes_itr = _votes.find( proposal_name.value );
    auto proposals_itr = _proposals.find( proposal_name.value );

    check( votes_itr != _votes.end(), "[proposal_name] votes does not exist");
    check( vote == "yes"_n || vote == "no"_n || vote == "abstain"_n, "[vote] invalid (ex: yes/no/abstain)");
```

修复情况：在 commit 031b72533a375c0aa22965debf2fcfa658567a7f 中修复。

6.5 提升建议

提升建议是对代码实现逻辑上的优化建议，项目方可根据实际情况进行相应的优化。

6.5.1 逻辑缺陷

(1) 在 complete 文件中，如果长时间无人调用 `complete()` 函数，比方说 1 年，下一个调用的人需要连续多次调用 `complete()` 函数才能激活提案或进行其他操作。

```
[[eosio::action]]
void wps::complete( )
{
    // no authorization required (can be executed by any account)

    // is contract paused or not
    check_contract_active();

    // check if current voting period is completed
    check( is_voting_period_complete(), "[current_voting_period] is not completed");
```

```
    // check if account has enough funding
    check_available_funding();

    // update `votes` from eligible voters
    // any existing votes with voters with less than 100 EOS vpay will be removed
    refresh_proposals();

    // update `proposals::eligible` field for all active proposals
    update_eligible_proposals();

    // payouts of active proposals
    handle_payouts();

    // set pending proposals to active status
    set_pending_to_active();

    // update current & next voting period
    update_to_next_voting_period();

    // re-update `proposals::eligible`
    update_eligible_proposals();
}
```

修复情况：在 commit c31333a3c2959c14e56d8ae1fc6a3f634930b8d3 中修复。

(2) 当调用 `complete()` 函数时，如果一个提案是符合条件但系统资金不足时，提案会被设置成 `expired`。

```
void wps::handle_payouts()
{
    // settings
    auto settings = _settings.get();
    auto state = _state.get();

    // static actions
    wps::claim_action claim( get_self(), { get_self(), "active"_n });

    // iterate proposals by active status
    for ( auto proposal_name : group_proposals( "active"_n ) ) {
```

```
        auto proposals_itr = _proposals.find( proposal_name.value );
        const eosio::asset monthly_budget = proposals_itr->monthly_budget;

        // only payout eligible (true) proposals
        if ( proposals_itr->eligible ) {

            // check internal available funding
            check( state.available_funding >= monthly_budget, "insufficient `available_funding`");
            sub_funding( monthly_budget );

            // update proposal payouts
            _proposals.modify( proposals_itr, same_payer, [&]( auto& row ) {
                row.payouts += monthly_budget;
            });
        } else {
            // remove proposal that no longer met threshold, cancel all subsequent proposals
            _proposals.modify( proposals_itr, same_payer, [&]( auto& row ) {
                row.status = "expired"_n;
            });
        }

        // set proposals to `completed/partial/expired/active`
        update_proposal_status( proposal_name );
    }
}
```

修复情况：经与项目方确认后，确认系统设计如此。

(3) complete.cpp 文件中 `update_eligible_proposals()` 函数在 `complete()` 函数中执行了 2 次。

```
[[eosio::action]]
void wps::complete( )
{
    // no authorization required (can be executed by any account)

    // is contract paused or not
    check_contract_active();

    // check if current voting period is completed
    check( is_voting_period_complete(), "[current_voting_period] is not completed");

    // check if account has enough funding
```

```
    check_available_funding();

    // update `votes` from eligible voters
    // any existing votes with voters with less than 100 EOS vpay will be removed
    refresh_proposals();

    // update `proposals::eligible` field for all active proposals
    update_eligible_proposals();

    // payouts of active proposals
    handle_payouts();

    // set pending proposals to active status
    set_pending_to_active();

    // update current & next voting period
    update_to_next_voting_period();

    // re-update `proposals::eligible`
    update_eligible_proposals();
}
```

修复情况：在 commit 073eff02c4706f94dee4df9c9ff17ef581ae67c2 中修复。

6.5.2 symbol 硬编码

(1) 代码中的硬编码的 `EOS` 应替换成 CORE_SYMBOL 以便在不同的链下进行方便的调试

修复情况：在 commit 8f77df700c3e4686d43bb06f95b452a108adbb5a 中修复。

慢雾科技
slow mist

官方网址

www.slowmist.com

电子邮箱

team@slowmist.com

微信公众号