SimplyVitalHealth Contract Audit

by Hosho, November 2017

Table of Contents

Technical Summary

This document outlines the overall security of HealthDRS system as evaluated by Hosho's Smart Contract auditing team.

The scope of this audit was to analyze and document SimplyVitalHealth's contract codebase for quality, security, and correctness.

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, merely an assessment of its logic and implementation. In order to ensure a secure contract that's able to withstand the Ethereum network's fast-paced and rapidly changing environment, we at Hosho recommend that the SimplyVitalHealth Team put in place a bug bounty program to encourage further and active analysis of the smart contract.

Auditing Strategy and Techniques Applied

The Hosho Team has performed an initial review of the smart contract code as written on October 19, 2017. The following contract files and their respective SHA256 fingerprints were evaluated:

Orignal Files	**Fingerprint (SHA256)**
transmute/contracts/BurnableToken.sol	`e5db698cd140ea4c184adc3fb2daefec9354eb25394be034907722c9b147e83d`
drs/contracts/HealthDRS.sol	`8616351cd7ffe584891b23a90ad942ff9120034c19f9bba8b93521f6b0f56510`
transmute/contracts/TransmuteAgent.sol	`8482b625ded9118b372199d0668449bdc11a2311aebac05c8b958dc9b0cf3477`

We completed a secondary review of the final edits to the code submitted on November 15, 2017. Those contract files and their respective SHA256 fingerprints are as follows:

Updated Files	**Fingerprint (SHA256)**

contracts/BurnableToken.sol	e5db698cd140ea4c184adc3fb2daefec9354eb25394be034907722c9b147e83d
contracts/HealthDRS.sol	6ed72029309b7784f4e3aad35b1c267479c24c560eaf278fb2fe4709857f92b1
contracts/TransmuteAgent.sol	8482b625ded9118b372199d0668449bdc11a2311aebac05c8b958dc9b0cf3477

Throughout the review process, care was taken to ensure that the token contract:

- Implements and adheres to existing ERC20 Token standard appropriately and effectively;
- Documentation and code comments match logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices in efficient use of gas, without unnecessary waste; and
- Uses methods safe from reentrance attacks.

The Hosho Team has followed best practices and industry-standard techniques to verify the implementation of SimplyVitalHealth's contract. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as they were discovered. Part of this work included writing a unit test suite using the Truffle testing framework. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

1. Due diligence in assessing the overall code quality of the codebase.
2. Cross-comparison with other, similar smart contracts by industry leaders.
3. Testing contract logic against common and uncommon attack vectors.
4. Thorough, manual review of the codebase, line-by-line.
5. Deploying the smart contract to testnet and production networks using multiple client implementations to run live tests.

Contract Analysis and Test Results

Summary

The HealthDRS contracts provided involve a raw ERC-20 token, used as a placeholder, as well as a Transmute contract, which exists for the purpose of issuing events to convert the tokens from the HealthDRS token to their side-chain in a clean manner, by burning the ERC-20 token. The HealthDRS contract makes up the majority of the work, and serves as a tracking system for URL's (Services), and keys that generate events when issued/etc.

There has been a small increase in coverage and branching as there are more executable portions of the contract. We're pleased to state that all uncovered paths, those that do not appear in the coverage report, have been manually verified. These cover systems like the address recovery (ecrecover wrapper) and the hard revert on the fallback function that require specific states to be applied.

Coverage Report

As part of our work assisting SimplyVitalHealth in verifying the correctness of their contract code, our team was responsible for writing a unit test suite using the Truffle testing framework.

The resulting code coverage (i.e., the ratio of tests-to-code) is as follows:

File	% Statements	% Branches	% Functions	% Lines
transmute/contracts/BurnableToken.sol	100.00%	100.00%	100.00%	100.00%
drs/contracts/HealthDRS.sol	95.88%	89.06%	95.24%	96.46%
transmute/contracts/TransmuteAgent.sol	100.00%	83.33%	100.00%	100.00%
All Files	**96.43%**	**88.57%**	**95.92%**	**96.92%**

Test Results

contract: erc-20 compliant token

✓ should allocate tokens per the minting function, and validate balances (152ms)

✓ should transfer tokens from 0x1bbb1269032bfd0b0fe0851235fc798af6bd3c9b to 0x42adbad92ed3e86db13e4f6380223f36df9980ef (75ms)

✓ should not transfer negative token amounts

✓ should not transfer more tokens than you have

✓ should allow 0x3b44fa9f7511113a8c1a1528070d45b1d7cdd101 to authorize 0x341106cb00828c87cd3ac0de55eda7255e04933f to transfer 1000 tokens (38ms)

✓ should not allow 0x3b44fa9f7511113a8c1a1528070d45b1d7cdd101 to authorize 0x341106cb00828c87cd3ac0de55eda7255e04933f to transfer an additional 1000 tokens once authorized, and authorization balance is > 0

✓ should allow 0x3b44fa9f7511113a8c1a1528070d45b1d7cdd101 to zero out the 0x341106cb00828c87cd3ac0de55eda7255e04933f authorization (42ms)

✓ should allow 0xdaef8d8c30eeb858b8c774a8d7d5e92a552bb0d9 to authorize 0x53353ef6da4bbb18d242b53a17f7a976265878d5 for 1000 token spend, and 0x53353ef6da4bbb18d242b53a17f7a976265878d5 should be able to send these tokens to 0x341106cb00828c87cd3ac0de55eda7255e04933f (99ms)

✓ should not allow 0x53353ef6da4bbb18d242b53a17f7a976265878d5 to transfer negative tokens from 0xdaef8d8c30eeb858b8c774a8d7d5e92a552bb0d9

contract: transmute

✓ should not set the token to burnableinstance with settokentotransmute using non-owner

✓ should set the token to burnableinstance with settokentotransmute (42ms)

✓ should instantiate contract with transmutenonce set to 0

✓ should not be able to call enable with non-owner

✓ should not be able to call transmutetoken with value greater than allowance (43ms)

✓ should not be able to call transmutetoken when enabled is false (39ms)

✓ should set boolean enable to true (39ms)

✓ should transmutetoken when boolean enabled is true (109ms)

contract: healthdrs

✓ should instantiate contract with owner set to accounts[0]

✓ should not allow transfer of ownership unless done by owner

✓ should not allow transfer of ownership to null account by a non-owner

✓ should not allow transfer of ownership to null account by the owner

✓ should allow transfer of ownership (84ms)

✓ should instantiate contract with burnable token

✓ should instantiate contract with latestcontract set to hlthdrsinstance.address

✓ should instantiate contract with version set to 1

✓ should not allow iskeyowner to be called with an invalid, null key

✓ should not allow isserviceowner to be called with an invalid, null service

✓ should not allow geturl to be called with an invalid, null service

✓ should not allow geturlfromkey to be called with an invalid, null key

✓ should not allow sethealthcashtoken to be called by non-owner with a standardtoken contract

✓ should allow sethealthcashtoken to be called by owner with a standardtoken contract (38ms)

✓ should return the token allowance for msg.sender

✓ should not allow setlatestcontract to be called by non-owner

✓ should allow setlatestcontract to be called by owner with the latest contract (103ms)

✓ should allow createservice to be called (72ms)

✓ should return the url associated with a service when geturl is called

✓ should return true when iskeyowner is called for an owned key

✓ should not allow createservice to be called for existing url

✓ should not allow createkey to be called by non-owner

✓ should not allow issuekey to be called by non-service owner

✓ should allow issuekey to be called (77ms)

✓ should allow createkey to be called, creating a new key (62ms)

✓ should return the url associated with a key when geturlfromkey is called
✓ should allow service owner to update a url with updateurl (135ms)
✓ should return true when iskeyowner is called for an owned key
✓ should not allow for sharekey to be called by non-key owner (41ms)
✓ should not allow for sharekey to be called when boolean canshare is false (46ms)
✓ should not allow for shareservice to be called from non-service owner account (38ms)
✓ should not allow for unsharekey to be called from non-key owner account (39ms)
✓ should not allow for unshareservice to be called from non-service owner account
✓ should not allow for createsalesoffer to be called from non-key owner account (38ms)
✓ should not allow for createsalesoffer to be called when boolean cansell is false (42ms)
✓ should not allow for cancelsalesoffer to be called from non-key owner account
✓ should not allow for purchasekey to be called when boolean cansell is false
✓ should not allow for tradekey to be called by non-key owner (40ms)
✓ should not allow for createtradeoffer to be called by non-key owner (48ms)
✓ should not allow for tradekey to be called when boolean cansell is false (76ms)
✓ should not allow for createtradeoffer to be called when boolean cansell is false (46ms)
✓ should not allow for setkeypermissions to be called with invalid key
✓ should not allow for setkeypermissions to be called by non-key owner (47ms)
✓ should return the length of the servicelist array
✓ should return the length of the keylist array
✓ should not allow for setkeypermissions to be called by non-key owner
✓ should return service url and owner when getservice is called
✓ should not allow for setkeypermissions to be called by non-key owner
✓ should return the service_id and owner for a key
✓ should not allow for setkeydata to be called for invalid key
✓ should not allow for setkeydata to be called by non-service owner (42ms)
✓ should return the length of the keylist array (73ms)
✓ should not allow for getkeydata to be called by invalid key
✓ should not allow for logaccess to be called with invalid key

✓ should not allow for logaccess to be called by non-service owner
✓ should call logaccess and record sent data in access event (87ms)
✓ should call message and record sent data in access event (63ms)
✓ should call message and record sent data in access event using service_id (51ms)
✓ should not call message and record sent data in for null address (40ms)
✓ should not allow for message to be called by non key and non-service owner (42ms)
✓ should not allow for log to be called by non key and non-service owner
✓ should call log and record sent data in access event (42ms)
✓ should call log and record sent data in access event for a service_id (41ms)
✓ should allow key owner to setkeypermissions (168ms)
✓ should allow key owner to authorize another account with the sharekey function (104ms)
✓ should not allow the same account to be shared with multiple times (99ms)
✓ should return false for iskeyowner with non-owner account
✓ should allow service owner to authorize another account with the shareservice function (88ms)
✓ should not allow service owner to authorize the same account with the shareservice function (88ms)
✓ should return false for isserviceowner with non-owner account (39ms)
✓ should allow key owner to deauthorize another account with the unsharekey function (276ms)
✓ should allow service owner to deauthorize another account with the unshareservice function (222ms)
✓ should allow key owner to create and cancel a sales offer for an owned key (155ms)
✓ should allow key owner to create a sales offer and buyer to purchase an owned key (443ms)
✓ should not allow anyone but the buyer to use a salesoffer (167ms)
✓ should allow createkey to be called (77ms)
✓ should not allow tradekey to be called when cantrade is false for the want key (81ms)
✓ should not allow createtradeoffer to be called when cantrade is false for the want key (67ms)
✓ should allow key owner to create and execute a trade (308ms)

✓ should allow createkey to be called (70ms)

✓ should not allow a trade offer where the key is not the wanted one (209ms)

✓ should call log and record sent data in access event (47ms)

✓ should not accept eth transfers

✓ should allow the owner to retrieve tokens that are trapped (95ms)

contract: ownable

✓ should instantiate contract with owner set to accounts[0]

✓ should not allow transfer of ownership unless done by owner

✓ should not allow transfer of ownership to null account by a non-owner

✓ should not allow transfer of ownership to null account by the owner

✓ should allow transfer of ownership (53ms)

Structure and Organization of Document

For ease of navigation, sections are arranged from most critical to least critical. Issues are tagged "Resolved" or "Unresolved" depending on whether they have been fixed or addressed. Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

- **Informational** - The issue has no impact on the contract's ability to operate.
- **Low** - The issue has minimal impact on the contract's ability to operate.
- **Medium** - The issue affects the ability of the contract to operate in a way that doesn't significantly hinder its behavior.
- **High** - The issue affects the ability of the contract to compile or operate in a significant way.
- **Critical** - The issue affects the contract in such a way that funds may be lost, allocated incorrectly, or otherwise result in a significant loss.

Complete Analysis

Resolved, Critical: Unable to Send Data Using Message Function

Explanation

A service is unable to send data via the `message` function, as `isKeyOwner` will throw an exception, as the from value should never be a valid key, except in the case of a hash collision, due to this, service owners are unable to send messages.

Resolution

A pre-check was added to the key so that it will only check if it is owned if the key is valid, preventing the exception while retaining the ownership check.

Resolved, Critical: Unable to Send Data Using Log Function

Explanation

A service is unable to send data via the the `log` function, as `isKeyOwner` will throw an exception, as the from value should never be a valid key, except in the case of a hash collision, due to this, service owners are unable to send messages.

Resolution

A pre-check was added to the key so that it will only check if it is owned if the key is valid, preventing the exception while retaining the ownership check.

Resolved, High: createService Function is Unprotected

Explanation

The `createService` function is not protected, and costs nothing to execute, there is nothing to stop someone from mass-spamming URI's into this and locking out URI's that may need to be transferred to someone else, and there is nothing stopping someone from simply executing, generating URI's, then throwing away the account. As the service key is a SHA-3 sum, it is extremely unlikely that a hash collision would occur, but it would be good practice to have some way to clean up this data.

Resolution

The contract is intended for open use by the developer community so needs to be a publicly accessible function. To address the issue of locking out urls, the service id is now calculated using both the url and msg.sender as this will prevent specific urls from becoming unusable.

Resolved, Medium: Very few protections to ensure key ownership

Example: I could offer to sell a key, setting the `canTrade` value to true, at which point, it could be sold, then I could execute `tradeKey` with a prearranged trade that puts the key back under my control.

Explanation

When keys are transferred, they should be locked down and secured. Extra owners removed, all valid trade/sell states cleared, etc. As it stands, it's possible to sell/trade/handle keys, then "take" them back if you're fast on the chain and/or your partner doesn't perform due diligence. It's also possible to set up a sale in advance, trade the key, then purchase it back immediately because `cancelSalesOffer` isn't called after a trade is complete. Again, there are multiple paths for this, and the full flow and possible stops need to be mapped out.

Resolution

Creating a salesOffer would cancel a tradeOffer and visa-versa so that you could only have one active at any given time; however the format of the trade function was not consistent with the sales functions so that was unclear. To resolve this the following changes were made:

1. Refactored the trade function, creating a cancelTradeOffer function to make it clear when this is used.
2. Added an additional requirement to canSell and canTrade modifiers, namely that the key must not be shared at all.
3. Added cancelSalesOffer to the createTradeOffer function and to the end of the purchaseKey function.
4. Added cancelTradeOffer to the createSalesOffer function and to the end of the tradeKey function.

This should accomplish the following: Only unshared keys can be sold or traded. There can only be an active sales offer. Or an active trade offer - never both. Completing a sale or trade - removes that sale or trade offer.

Resolved, Medium: No Fallback Function

Explanation

The contract should have a fallback function, even if it contains nothing more than a `revert()` in order to ensure ETH isn't accidentally sent and trapped in the contract.

Resolution

Fallback function with revert added

Resolved, Low: No Self Destruct

Explanation

As this contract could potentially become quite large over time because it is functionally being used as a database, we suggest considering the addition of a self-destruct capability in case you desire to eventually move this data off the block chain, and wish to remove the contract.

Resolution

As this contract is intended to be used by multiple service providers - having an `ownerOnly` self-destruct may preclude third-party use as the contract’s availability would not be guaranteed.

Closing Statement

We are grateful to have been given the opportunity to work with the SimplyVitalHealth team on this project and audit. They have been very receptive to our feedback and were agreeable in correcting the small numbers of issues found.

During the initial static analysis, several possible vulnerabilities were noted, and the SVH team was very quick to patch these and return the updated code. They implemented the required fixes to ensure the long-term health and stability of the HealthDRS system as it works within the Ethereum ecosystem. It was also noted that there were some code paths that were not executable during dynamic testing and the SVH team corrected these to a functional state.

Even beyond the small issues found, the SVH team implemented some of our suggested improvements. We wish the SVH team well with the HealthDRS system going forwards.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them.

We at Hosho recommend that the SimplyVitalHealth Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.