Quantstamp Security Assessment Certificate

July 15th 2022 — Quantstamp Verified

Casper Signer (Phase 1)

This security review was prepared by Quantstamp, leaders in Blockchain security and solutions.

Executive Summary

Type	Browser Extension
Reviewers	Joseph Xu, Technical R&D Advisor Leo Antelyes, Fullstack Web Developer
Timeline	2021-05-03 through 2021-05-07
Languages	TypeScript
Methods	Black-Box Security Testing, Functional Testing
Specification	README.md
Documentation Quality	Low
Test Quality	Undetermined

Source Code

Repository	Commit
signer (v0.3.9)	d5fc914

Goals

- Test functionalities of the Casper Signer extension
- Identify potential threats to authentication or privilege escalation
- Identify potential threats that can lead to sensitive data being exposed
- Identify UI/UX elements that may inadvertently lead to security threats

Total Issues	**13**	(0 Resolved)
High Risk Issues	**2**	(0 Resolved)
Medium Risk Issues	**4**	(0 Resolved)
Low Risk Issues	**2**	(0 Resolved)
Informational Risk Issues	**3**	(0 Resolved)
Undetermined Risk Issues	**2**	(0 Resolved)

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
Informational	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
? Undetermined	The impact of the issue is uncertain.

Unresolved	Acknowledged the existence of the risk, and decided to accept it without engaging in special efforts to control it.
Acknowledged	The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).
Fixed	Adjusted program implementation, requirements or constraints to eliminate the risk.
Mitigated	Implemented actions to minimize the impact or likelihood of the risk.

Summary of Findings

Quantstamp has performed a black-box security review on the Casper Signer browser extension. Due to the nature of the black-box security review, Quantstamp assumed the following threat model:

- The attacker is able to access the user's OS session but not the browser extension session.
- The attacker has a basic knowledge of cryptocurrencies, blockchain, and web programming.
- The attacker is resource-constrained. This means that the attacker only has access to the user's OS session for a short time, will not run additional programs or scripts locally on the user's OS session (e.g., keylogger, screen recorder, remote-access trojan, etc.), and only has access to external resources such as the public repository of the Casper Signer or a simple web search.
- The user is not assumed to have the best security practices.

Based on the above threat model, Quantstamp has identified 13 issues in total, including several issues that may allow the attacker to easily access sensitive information or inadvertently lead to the loss of keys for the user. It is possible to strengthen the security of the extension by improving the data storage, session management, and UI/UX practices. We recommend that these issues be addressed, as improvements on these aspects can be highly effective in deterring simple attacks.

ID	Description	Severity	Status
QSP-1	Encrypted Vault and Password Salt Are Easily Accessible	︽ High	Unresolved
QSP-2	Signer Connection Is Established Globally to Multiple Sites	︽ High	Unresolved
QSP-3	Lack of Strong Password Policy Enforcement	^ Medium	Unresolved
QSP-4	Lack of Session Management	^ Medium	Unresolved
QSP-5	Account Removal Does Not Require the Vault Password	^ Medium	Unresolved
QSP-6	Private Key Can Be Revealed Without the Vault Password	^ Medium	Unresolved
QSP-7	Unlimited Retry Attempts for Unlocking the Extension	˅ Low	Unresolved
QSP-8	Extremely Easy to Reset the Vault	˅ Low	Unresolved
QSP-9	No Requirements on Valid Account Name	○ Informational	Unresolved
QSP-10	Lack of Validation When Importing an Account	○ Informational	Unresolved
QSP-11	The Signer Connection Prompt Is Not Informative Enough	○ Informational	Unresolved
QSP-12	Signer May Get Stuck on Vault Creation Screen after Declining Signature	? Undetermined	Unresolved
QSP-13	Downloaded Key Files Rely on Users for Secure Storage	? Undetermined	Unresolved

Quantstamp Review Breakdown

Quantstamp's objective was to evaluate the browser extension for security-related issues and best practices.

Possible issues we looked for included (but are not limited to):

- Authentication and access control
- Data storage best practices
- Input validations
- Session management best practices
- Business logic contradicting the specification

Methodology

The Quantstamp reviewing process follows a routine series of steps:

1. Application review that includes the following:
   i. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the application.
   ii. Comparison to specifications, which is the process of checking whether the application fulfills the functionalities and does what the specifications, sources, and instructions provided to Quantstamp describe.
   iii. A black-box security testing of the application, generally based on the OWASP Web Security Testing Framework.
2. Best practices review, which is a review of the input files to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
3. Specific, itemized, and actionable recommendations to help you take steps to secure your application.

Findings

QSP-1 Encrypted Vault and Password Salt Are Easily Accessible

Severity: *High Risk*

Status: Unresolved

Description: The Casper Signer extension stores the encrypted vault (containing serialized public and private keys) and password salt (for unlocking the Casper Signer) directly in the browser's local storage. This data persists in the browser extension page and is easily accessible. For example, an attacker can view these easily using the "Inspect" feature on the browser extension window, even when the app state is locked.

Exploit Scenario: An attacker can easily copy the encrypted vault data for further analysis at a later time. Combined with the lack of strong password policy enforcement, the attacker may be able to successfully crack the vaults of users through password brute-force attacks.

Recommendation: Do not store any sensitive data using the `localStorage` API. For Chrome, it is possible to use the `chrome.storage` API so that these sensitive data is not directly visible using the browser's "Inspect" feature (as is done in Metamask). Ideally, the data is preserved on disk and is read to/cleared from memory on every unlock/lock event.

QSP-2 Signer Connection Is Established Globally to Multiple Sites

Severity: *High Risk*

Status: Unresolved

Description: Casper Signer establishes connections to multiple sites with a single approval. For example, a user can approve connection to `https://cspr.live/`. If the user then opens `https://clarity-testnet-old.make.services/` in a new tab, Casper Signer is automatically connected to the new site even though connection has not been explicitly approved by the user. Furthermore, the Signer also indicates that it remains in the "Connected" status on any other website visited afterwards.

Exploit Scenario: A malicious site may exploit the current connection model to track a user by public key upon access or generate unwanted signature requests. While the threat may be minimal at this point due to the limited number of sites that have Casper Signer integration, it may become a bigger threat in the future.

Recommendation: Develop a more granular management of connections so that Casper Signer is only connected to a site after explicit user approval.

QSP-3 Lack of Strong Password Policy Enforcement

Severity: *Medium Risk*

Status: Unresolved

Description: There are no restrictions on the password that is used to unlock the extension. Simple passwords, such as "pass", "a", "123", and "[empty spaces]", are all considered valid passwords when setting up a vault. The lack of strong password policy faciliates brute force attacks.

Recommendation: Enforce strong password policy when setting up the vault. We strongly suggest following the NIST Digital Identity Guidelines or OWASP Authentication Cheatsheet for implementing a strong password policy. Furthermore, inform users of the requirements of a strong password in the front-end.

QSP-4 Lack of Session Managaement

Severity: *Medium Risk*

Status: Unresolved

Description: The browser extension does not lock automatically after a period of inactivity or OS screen lock. Combined with the lack of password requirement for highly sensitive operations (account removal or generating the private key file), this makes the Casper Signer highly vulnerable if the user inadvertently forgets to manually lock the extension and leaves the computer unattended for some time.

Exploit Scenario: Add a session management feature that locks the extension if it is left inactive (e.g., focus lost) for a certain period or if the screen is locked from the OS side. Users can be allowed to configure how long a session should last.

QSP-5 Account Removal Does Not Require the Vault Password

Severity: *Medium Risk*

Status: Unresolved

Description: The user can remove an account (inadvertently or not) without being prompted for the vault password. An attacker can remove accounts easily if the user leaves the browser extension unlocked.

Recommendation: Prompt users to input the vault password before removing an account.

QSP-6 Private Key Can Be Revealed Without the Vault Password

Severity: *Medium Risk*

Status: Unresolved

Description: The user can generate files containing an account's private key without being prompted for the vault password. An attacker can easily access an account's private key if the user leaves the browser extension unlocked.

Recommendation: Prompt users to input the vault password before generating the files containing an account's private and public keys.

QSP-7 Unlimited Retry Attempts for Unlocking the Extension

Severity: *Low Risk*

Status: Unresolved

Description: An attacker has unlimited number of attempts to try and unlock the Casper Signer manually. Combined with the lack of strong password policy enforcement, some users may have Vaults that are vulnerable to simple brute-force attacks.

Recommendation: Consider putting the Casper Signer into a lockdown state for a limited time (e.g., 10 minutes) if too many unsuccessful attempts to unlock the extension have been made (e.g., 10 tries).

QSP-8 Extremely Easy to Reset the Vault

Severity: *Low Risk*

Status: Unresolved

Description: The user can reset the entire Vault while Casper Signer is locked by clicking on the "Reset Vault" button. This will delete all accounts currently associated with the Casper Signer extension. An attacker can simply reset the entire vault and cause damage to the user if the accounts and associated keys have not been backed up.

Recommendation: Require either the Vault password or a valid public-private key pair (that will be imported into Casper Signer as an account in the new Vault) to reset the vault. While the latter does not prevent the attacker from resetting the entire vault, it creates an additional hurdle compared to the current situation in which a complete reset takes only two clicks.

QSP-9 No Requirements on Valid Account Name

Severity: *Informational*

Status: Unresolved

Description: There are no restrictions on the account name associated with a signing key pair. Names such as "[empty spaces]", ",", "." are all considered valid account names.

Recommendation: Consider allowing only human readable account names consisting of alphanumeric characters above a minimum length.

QSP-10 Lack of Validation When Importing an Account

Severity: *Informational*

Status: Unresolved

Description: There is no file extension or size validation when importing an account from a downloaded private key file. While there is validation of encoding, misuse of this feature (e.g., reading in a very large file) may cause the browser to crash.

Recommendation: Allow only files with the correct extension to be selected in the file browser. In addition, add a cap to the allowed file size.

QSP-11 The Signer Connection Prompt Is Not Informative Enough

Severity: *Informational*

Status: Unresolved

Description: Whenever a user attempts to establish a connection to a site using Casper Signer, the prompt only asks "Connect Signer to site?" without specifying which site.

Recommendation: Include additional information in the prompt so that the user can tell which site is requesting connection.

QSP-12 Signer May Get Stuck on Vault Creation Screen after Declining Signature

Severity: *Undetermined*

Status: Unresolved

Description: If a signing request is declined, the Casper Signer may get stuck on the initial setup screen that prompts the user to create a new vault. The browser session must be restarted to fix this.

We note that while it is not possible to create a new vault, this screen could be alarming to users. If the new vault creation does go through, users may risk losing the original vault and its associated keys.

Recommendation: Ensure that the Casper Signer returns to the home screen after declining a signing request.

QSP-13 Downloaded Key Files Rely on Users for Secure Storage

Severity: *Undetermined*

Status: Unresolved

Description: Casper Signer allows users to generate and download files that contain the private and public keys of an account. The files are in plaintext and clearly indicates that these are the private and public keys within the file. Attackers can easily gain access to the private key from these files (e.g., by searching the file system) if the user has little security awareness or has bad security practice.

Recommendation: When a user tries to generate the files containing the keys, show a prompt to remind the security implications of this action. Furthermore, create a user-facing documentation to provide guidance on how to properly secure the private key.

Adherence to Best Practices

- The terminologies used in the UI are unclear as multiple terms seem to refer to the same concept. For example, "private key"/"secret key" seem to be used interchangeably as are "account"/"account key"/"key". We recommend better organization of terminologies the UI so that different words always refer to different concepts.
- When a user generates the files associated with an active key, the public key is logged to the console. We recommend avoiding unnecessary logging.
- The following deprecation warning has been noted on the console.

```
2.601d8adb.chunk.js:2 [Deprecation] SharedArrayBuffer will require cross-origin isolation as of M91, around May 2021. See https://developer.chrome.com/blog/enabling-shared-array-buffer/ for more details.
```

Changelog

- 2021-05-07 - Initial report

About Quantstamp

Quantstamp is a Y Combinator-backed company that helps to secure blockchain platforms at scale using computer-aided reasoning tools, with a mission to help boost the adoption of this exponentially growing technology.

With over 1000 Google scholar citations and numerous published papers, Quantstamp's team has decades of combined experience in formal verification, static analysis, and software verification. Quantstamp has also developed a protocol to help smart contract developers and projects worldwide to perform cost-effective smart contract security scans.

To date, Quantstamp has protected $5B in digital asset risk from hackers and assisted dozens of blockchain projects globally through its white glove security assessment services. As an evangelist of the blockchain ecosystem, Quantstamp assists core infrastructure projects and leading community initiatives such as the Ethereum Community Fund to expedite the adoption of blockchain technology.

Quantstamp's collaborations with leading academic institutions such as the National University of Singapore and MIT (Massachusetts Institute of Technology) reflect our commitment to research, development, and enabling world-class blockchain security.

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by Quantstamp; however, Quantstamp does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication.

Notice of confidentiality

This report, including the content, data, and underlying methodologies, are subject to the confidentiality and feedback provisions in your agreement with Quantstamp. These materials are not to be disclosed, extracted, copied, or distributed except to the extent expressly authorized by Quantstamp.

Links to other websites

You may, through hypertext or other computer links, gain access to web sites operated by persons other than Quantstamp, Inc. (Quantstamp). Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites' owners. You agree that Quantstamp are not responsible for the content or operation of such web sites, and that Quantstamp shall have no liability to you or any other person or entity for the use of third-party web sites. Except as described below, a hyperlink from this web site to another web site does not imply or mean that Quantstamp endorses the content on that web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the report. Quantstamp assumes no responsibility for the use of third-party software on the website and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.