VIBRANIUM AUDITS

Security Assessment

aeternity-snap

Verified by Vibranium Audits on 13 March 2024

Vibranium Audits Verified on February 17th, 2024

Aeternity Snap

The security assessment was prepared by Vibranium Audits.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Metamask Snap	N/A	Manual Review, penetration testing and Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
TypeScript	Delivered on 18/03/2024	N/A
CODEBASE		**COMMITS**
JavaScript		1c93bdb2e29572dc91b69b16f3db7b5bdae5822c

Vulnerability Summary

4	0	0	0	4	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

0 Critical	0 Resolved	Critical vulnerabilities are usually straightforward to exploit and can lead to the loss of user funds or contract state manipulation by external or internal actors.
1 High	0 Resolved	High vulnerabilities are usually harder to exploit, requiring specific conditions, or have a more limited scope, but can still lead to the loss of user funds or contract state manipulation by external or internal actors.
3 Medium	0 Resolved	Medium vulnerabilities are usually limited to state manipulations, but cannot lead to assets loss. Major deviations from best practices are also in this category.
0 Low	0 Resolved	Low vulnerabilities are related to outdated and unused code or minor gas optimization. These issues won't have a significant impact on code execution, but affect the code quality.
0 Informational	0 Resolved	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | Aeternity Snap

CODEBASE | Aeternity Snap

Repository

https://github.com/4-point-0/aeternity-snap/

Commits

1c93bdb2e29572dc91b69b16f3db7b5bdae5822c

APPROACH & METHODS | Aeternity Snap

This report has been prepared for Aeternity Snap(2024) to discover issues and vulnerabilities in the source code of the Aeternity Snap project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Manual Review, rigorous Penetration Testing and Static Analysis techniques.

The auditing process pays special attention to the following considerations:

- Pen-Testing the Snaps against both common and uncommon attack vectors.
- Assessing the code base to ensure compliance with current best practices and industry standards
- Ensuring Snap logic meets the specifications and intentions of the client.
- Thorough line-by-line manual review of the entire code base by industry experts.

The security assessment resulted in findings that ranged from critical to informational We recommend addressing these findings to ensure a high level of security standards and industry practices.
We suggest recommendations that could better serve the project from the security perspective:

- Testing the Snap against both common and uncommon attack vectors.
- Enhance general coding practices for better structures of source codes.
- Review unit tests to cover the possible use cases.
- Review functions for readability, especially for future development work.

FINDINGS | Aeternity Snap

4	1	3	0	0
Total Findings	High	Medium	Low	Informational

This report has been prepared to discover issues and vulnerabilities for Aeternity snap. Through this audit, we have uncovered 4 issues ranging from different severity levels. Utilizing the techniques of Manual Review, Penetration Testing & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

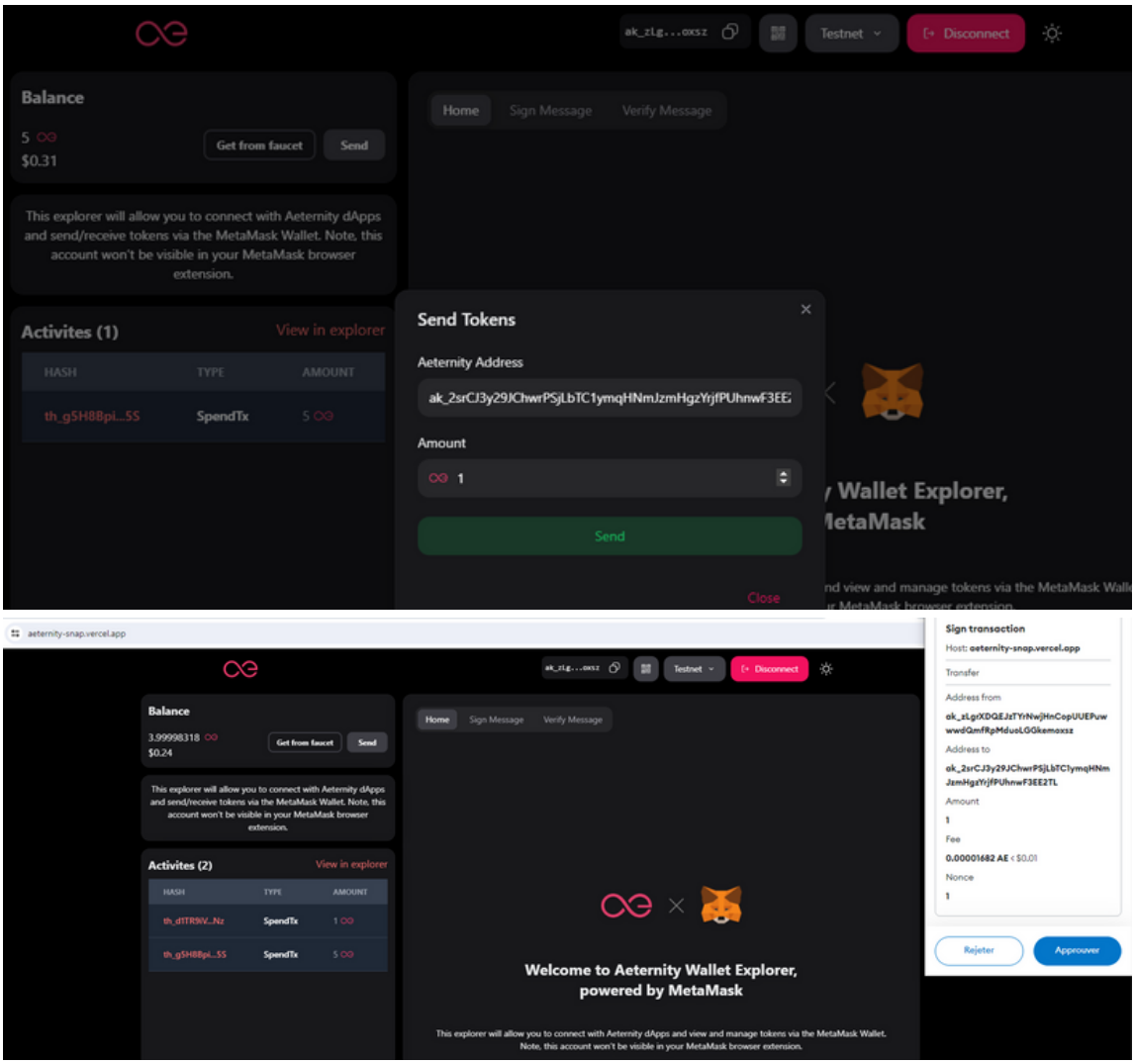
ID	Title	Category	Severity	Status
VA-01	Unhandled confirmation	Design Issue	Medium	Acknowledged
VA-02	Dapp May Suppress User Confirmation	Design Issue	Medium	Acknowledged
VA-03	Superfluous Permission	Design Issue	High	Acknowledged
VA-04	Vulnerable Outdated dependency	Design Issue	Medium	Acknowledged

VA-01 | Unhandled confirmation

Category	Severity	Location	Status
Design Issue	Medium	1c93bdb2e29572dc91b69b16f3db7b5bdae5822c	Acknowledged

Description

For key Snap functionalities (such as transferring funds or signing of a message), dialogs are displayed for the user to confirm whether they are aware of what they are doing. If the user confirms the transaction, it is executed. The snap in the send tokens functionality perform the action without the confirmation from the user. In case the user made a mistake and want to cancel the transfer it won't be possible. The confirmation pop up shows but the transaction is already being processed .



Recommendation

Handle the confirmation dialog before processing the user action.

VA-02 | Dapp May Suppress User Confirmation

Category	Severity	Location	Status
Design Issue	Medium	1c93bdb2e29572dc91b69b16f3db7b5bdae5822c	Acknowledged

Description

The dapp controls if the user is requested confirmation to return the public key. If the dapp sets confirm=false the user will not be informed that the dapp accessed their pubkey information (any account). Allowing the dapp to control if the user is asked to extract certain (derived) information from the snap is intransparent and may leak sensitive information. Especially in a setting where the snap is gatekeeping access to user specific information.

aeternity-snap / packages / snap / src / index.ts

Code | Blame | 128 lines (109 loc) · 3.33 KB

```
24  module.exports.onRpcRequest = async ({ origin, request }: any) => {
30
31    switch (request.method) {
32      case "getPublicKey": {
33        const { derivationPath, confirm = false } = request.params || {};
34
35        assertIsBoolean(confirm);
36
37        const keyPair = await deriveKeyPair(derivationPath);
38        const publicKey = encodePublicKey(keyPair.publicKey);
39
40        if (confirm) {
41          const accepted = await renderGetPublicKey(
42            dappHost,
43            "Are you sure you want to get account address?",
44          );
45          assertConfirmation(accepted);
46        }
```

Recommended

The snap should strictly enforce user confirmation on the first time the pubkey is requested from an origin. A potentially untrusted dapp (even though origin restricted; a dapp might turn malicious and should therefore be treated as untrusted) should never be able to silently dictate what security measures be enabled with a snap request.

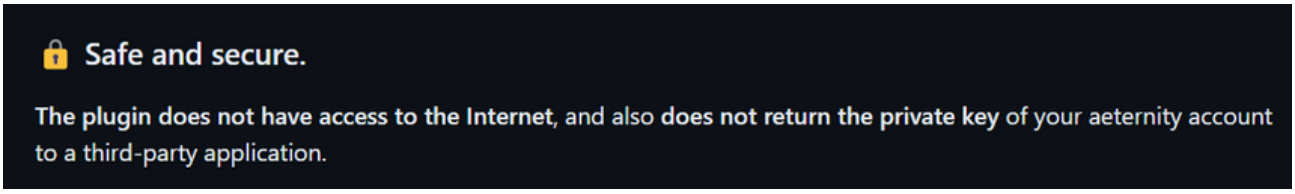
VA-03 | Superfluous Permission

Category	Severity	Location	Status
Design Issue	High	1c93bdb2e29572dc91b69b16f3db7b5bdae5822c	Acknowledged

Description

The snap requests permission endowment:network-access to interact with external entities over HTTP/fetch. While in the dApp repository it is written explicitly that the plugin does not have access to the internet, the dApp requests access to internet in order to continue using it.
The screenshot was taken from:
aeternity-snap/packages/snap/snap.manifest.json

```
26        },
27        "endowment:network-access": {},
28        "snap_getBip32Entropy": [
```



Recommended

Remove superfluous permissions.

VA-04 | Vulnerable Outdated dependency

Category	Severity	Location	Status
Design Issue	Medium	1c93bdb2e29572dc91b69b16f3db7b5bdae5822c	Acknowledged

Description

The snap uses a has a vulnerable dependency as described in package.json. The package postcss which version inferior to 8.4.31 is known to be vulnerable to 1 CVE. The package vulnerability details can be found under the reference CVE-2023-44270.

packages/site/package.json

```
38      "next": "^13.5.6",
39      "next-themes": "^0.2.1",
40      "nextjs-node-loader": "^1.1.5-alpha.0",
41      "postcss": "8.4.29",
42      "qrcode.react": "^3.1.0",
43      "react": "^18.2.0",
44      "react-dom": "^18.2.0",
```

GitHub Advisory Database / GitHub Reviewed / CVE-2023-44270

PostCSS line return parsing error

Moderate severity | GitHub Reviewed | Published on Sep 30, 2023 to the GitHub Advisory Database • Updated on Nov 5, 2023

Vulnerability details | Dependabot alerts 0

Package	Affected versions	Patched versions
postcss (npm)	< 8.4.31	8.4.31

Recommended

Remove unused dependencies, components and files.
Continuously inventory the versions of packages and monitor for any security updates especially.

DISCLAIMER | VIBRANIUM AUDITS

This report is subject to the terms and conditions (including without limitation description of services confidentiality disclaimer and limitation of liability) set forth in the Services Agreement or the scope of services and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement This report may not be transmitted disclosed referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Vibranium Audits prior written consent in each instance

This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team This report is not nor should be considered an indication of the economics or value of any “product” or “asset”created by any team or project that contracts Vibranium Audits to perform a security assessment This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed nor do they provide any indication of the technologies proprietors business business model or legal compliance

This report should not be used in any way to make decisions around investment or involvement with any particular project This report in no way provides investment advice nor should be leveraged as investment advice of any sort This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology

Blockchain technology and cryptographic assets present a high level of ongoing risk Vibranium Audits position is that each company and individual are responsible for their own due diligence and continuous security Vibranium Audits goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze

The assessment services provided by Vibranium Audits is subject to dependencies and under continuing development You Agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty The assessment reports could include false positives false negatives and other unpredictable results The services may access and depend upon multiple layers of third-parties

ALL SERVICES THE LABELS THE ASSESSMENT REPORT WORK PRODUCT OR OTHER MATERIALS OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND “AS AVAILABLE” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW VIBRANIUM AUDITS HEREBY DISCLAIMS ALL WARRANTIES WHETHER EXPRESS IMPLIED STATUTORY OR OTHERWISE WITH RESPECT TO THE SERVICES ASSESSMENT REPORT OR OTHER MATERIALS WITHOUT LIMITING THE FOREGOING VIBRANIUM AUDITS SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY FITNESS FOR A PARTICULAR PURPOSE TITLE AND NON-INFRINGEMENT AND ALL WARRANTIES ARISING FROM COURSE OF DEALING USAGE OR TRADE PRACTICE WITHOUT LIMITING THE FOREGOING VIBRANIUM AUDITS MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES THE LABELS THE ASSESSMENT REPORT WORK PRODUCT OR OTHER MATERIALS OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF WILL MEET CUSTOMER’S OR ANOTHER PERSON’S REQUIREMENTS ACHIEVE ANY INTENDED RESULT BE COMPATIBLE OR WORK WITH ANY SOFTWARE SYSTEM OR OTHER SERVICES OR BE SECURE ACCURATE COMPLETE FREE OF HARMFUL CODE

OR ERROR-FREE WITHOUT LIMITATION TO THE FORGOING, VIBRANIUM AUDITS PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KINDTHAT WILL MEET CUSTOMER' S REQUIREMENTS ACHIEVE ANY INTENDED RESULTS BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE APPLICATIONS SYSTEMS OR SERVICES OPERATE WITHOUT INTERRUPTION MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED

WITHOUT LIMITING THE FOREGOING NEITHER VIBRANIUM AUDITS NOR ANY OF VIBRANIUM AUDITS AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND EXPRESS OR IMPLIED AS TO THE ACCURACY RELIABILITY ORCURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE VIBRANIUM AUDITS WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS MISTAKES OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE OF ANY NATURE WHATSOEVER RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES ASSESSMENT REPORT OR OTHER MATERIALS

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNEROR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS

THE SERVICES ASSESSMENT REPORT AND ANY OTHER MATERIALS HERE UNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT NOR MAY COPIES BE DELIVERED TO ANY OTHER PERSON WITHOUT VIBRANIUM AUDITS PRIOR WRITTEN CONSENT IN EACH INSTANCE

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES ASSESSMENT REPORT AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST VIBRANIUM AUDITS WITH RESPECT TO SUCH SERVICES ASSESSMENT REPORT AND ANY ACCOMPANYING MATERIALS

THE REPRESENTATIONS AND WARRANTIES OF VIBRANIUM AUDITS CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER ACCORDINGLY NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST VIBRANIUM AUDITS WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE

FOR AVOIDANCE OF DOUBT THE SERVICES INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS ORMATERIALS SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Vibranium | Securing the Web3 World

Vibranium Audits is a blockchain security company that was founded in 2021 by professors from the University of Greenwich and cyber-security engineers from ITI Capital. As pioneers in the field, Vibranium Audits utilizes best-in-class Formal Verification and AI technology to secure and monitor blockchains, smart contracts, and Web3 apps.