// HALBORN

ANATHA WALLET

Penetration Test

Prepared by: **Halborn**
Date of Engagement: **10.07-16.2020**
Visit: **Halborn.com**

TABLE OF CONTENTS

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	10/08/2020	Steven Walbroehl
0.2	Document Edits	10/11/2020	Steven Walbroehl
1.0	Document Final	10/12/2020	Steven Walbroehl

CONTACTS

CONTACT	COMPANY	EMAIL
STEVEN WALBROEHL	Halborn	Steven.Walbroehl@halborn.com
ROB BEHNKE	Halborn	Rob.Behnke@halborn.com

1.1 INTRODUCTION

Anatha engaged Halborn to conduct a security assessment on their Desktop Client Wallet starting on October 7th, 2020 and ending October 16th, 2020. The security assessment was scoped to the functionality of the wallet, the security of the keys used, the connectivity It uses to get/post data to external APIs, and the overall security of the compiled code

The first round of testing uncovered several issues with the private key and how it was saved locally by the IndexedDB, as well as API keys being used to enable functionality from external services (such as etherscan.io and infura) The findings were acknowledged and addressed by the Anatha development team shortly following the disclosure of the Issues.

While both findings are mitigated; the Anatha team is in the process of implementing a caching layer on a new data exchange endpoint that the Desktop wallet interfaces with. The cache layer will allow keys to use the services of those endpoints in which Wallet functionality relies upon, and not potentially hit rate limits during high use. Infura has been placed on the caching layer with the other services scoped in this document underway. The final version of the application code will be revalidated and re-tested by Halborn security engineers after further updates are made.

Overall, the desktop wallet follows a high-quality software development standard, contains validated and strong encryption and hashing libraries to protect the users' keys, and functions as intended.

Halborn as determined the Desktop wallet to be secure from private key exposure and exploitation, but has a degree of risk still remaining in regards to availability communicating to third parties if rate limits are exceeded, which may impact functionality of several parts within the client software.

1.2 Test Approach & Methodology

Halborn performed a combination of manual and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of the penetration test. The majority of the time was spent evaluating its use of the mneumonic seed, and the protection of the private keys. The following phases and associated tools were used throughout the term of the audit:

- Research into architecture, purpose, and use of client wallet.
- Manual code read and analysis.
- Reverse engineering of the hashing and encryption functions used Inside the wallet.
- Scanning of code used to locate bugs or security flaws.(SONARQUBE)
- Proxying the traffic from the local client to the external Internet to determine the traffic and data leaving the system. (REDUX, POSTMAN, BURP SUITE)
- Uploading of Images and data files to see Input handling.
- Open source dependency versions and vulnerabilities.

1.3 Scope

IN-SCOPE:

Code related to the Desktop wallet, and the compiled binaries.

OUT-OF-SCOPE

External API's hosted by systems the wallet connects to, such as etherscan.io or Infura.

1.4 Version Tested

Git commit: e6971a912a37ec3b0c50469d282916657a78daed
Ver. - v0.20.107

1.4 ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW
0	1	1	1

SECURITY ANALYSIS	RISK LEVEL
API SERVICE RATE LIMITS MAY IMPACT FUNCTIONALITY	HIGH
VULNERABLE VERSIONS OF SEVERAL OPEN SOURCE PACKAGES	LOW
STORAGE AND HANDLING OF LOCAL PRIVATE KEYS	Informational
HRA	Informational

FINDINGS & TECH DETAILS

3.1 API SERVICE RATE LIMITS - HIGH

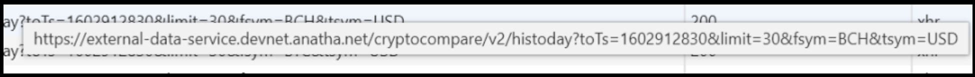
Description

The Anatha Wallet utilizes several third party API services to Integrate and provide functionality within the desktop client. Current version of the application tested (0.20.107) Interfaces with a data exchange layer at:

http://external-data-service.devnet.anatha.net

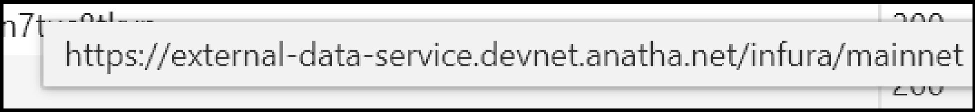
This layer is used to call to the third parties similar to a proxy so that clients do not call the API endpoints directly.
The tester observed that, while the application will function correctly with Individual use, denial of service conditions are likely to occur under times of high usage by many users of the desktop wallet at once. This Is due to rate-limits set by the third parties.
The services discovered and used include:

Cryptocompare:



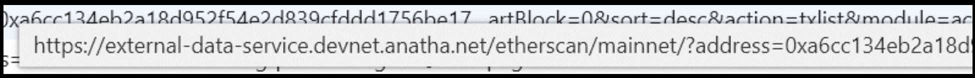
https://external-data-service.devnet.anatha.net/cryptocompare/v2/histoday?toTs=1602912830&limit=30&fsym=BCH&tsym=USD

Infura:



https://external-data-service.devnet.anatha.net/infura/mainnet

Etherscan:



https://external-data-service.devnet.anatha.net/etherscan/mainnet/?address=0xa6cc134eb2a18d

Changelly

Changenow

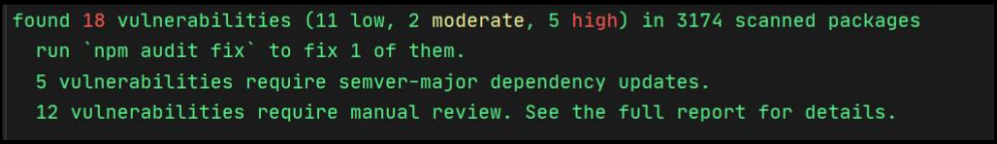
Recommendation

Anatha team is in the process of implementing a caching layer on a new data exchange endpoints Identified above. This cache layer will allow keys to use the services of those endpoints in which wallet functionality relies upon, and not potentially hit rate limits during high use. Currently infura has been placed on the caching layer with the other services scoped in this document underway. The final version of the application code will be revalidated and re-tested by Halborn security engineers after further updates are made.

3.2 VULNERABLE VERSIONS OF SEVERAL OPENSOURCE PACKAGES- LOW

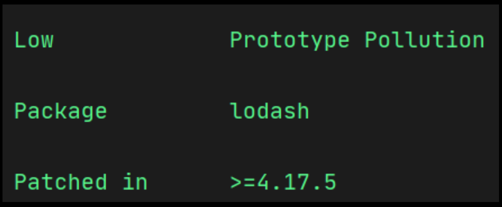
Description

Halborn used sourced the code from the Private GitHub to compile and view/test all dependencies and open source packages used. While nothing of critical risk is imported, the tester is noting several packages that (node/npm) came back with security potential issues.

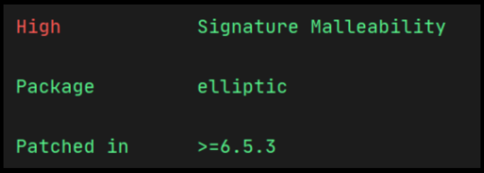


```
found 18 vulnerabilities (11 low, 2 moderate, 5 high) in 3174 scanned packages
  run `npm audit fix` to fix 1 of them.
  5 vulnerabilities require semver-major dependency updates.
  12 vulnerabilities require manual review. See the full report for details.
```

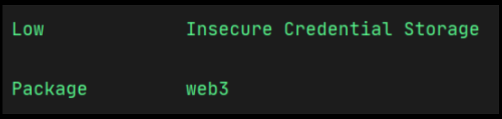
Among them are: node-fetch, elliptic, web3, js-yaml and lodash



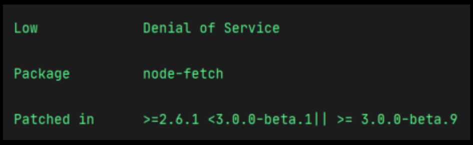
Low	Prototype Pollution
Package	lodash
Patched in	>=4.17.5



High	Signature Malleability
Package	elliptic
Patched in	>=6.5.3



Low	Insecure Credential Storage
Package	web3



Low	Denial of Service
Package	node-fetch
Patched in	>=2.6.1 <3.0.0-beta.1|| >= 3.0.0-beta.9

Recommendation

Consider either removing these packages if not needed from the compiled application, or upgrade them to secured version.

In the case of web3 Insecure Credential Storage, this is accepted to function properly. The credentials used IndexDB to sign transactions with the key stored locally.

3.2.2. STORAGE OF PRIVATE KEYS- INFORMATIONAL

Description

Halborn thoroughly tested the private key utilization of the wallet for any risk to exposure, theft, or loss.

This is an informational update for the reader validating that no exploitation opportunities were discovered during the assessment.

The main points validated are:

- KEYS SENT IN TRANSIT OFF THE CLIENT - NO

- KEYS STORED UNENCRYPTED LOCALLY - NO

- KEYS STORAGE LOCATION - INDEXDB

- STRONG KEY GENERATION LIBRARY - YES (crypto-js AES and EBK-DF2 for Hashing)

- STRONG PASSWORD IMPLEMENTATION - YES

Recommendation

While the locally stored file is encrypted that contains the credentials and keys used by IndexDB; the user should ensure this file still be properly protected with strong passwords. All technical mitigations have been provided by Anatha to protect the key.

3.2.3. HRA - INFORMATIONAL

Description

Halborn thoroughly tested HRA aspect used In the Wallet to generate profiles. Among the tests performed were:

- Injection techniques

- Image Metadata payloads (stegonagraphy)

- Client side exploitation

- Proxy Requests tampering

No Issues detected in HRA.

Recommendation

No issues detected in HRA component.

THANK YOU FOR CHOOSING

// HALBORN