SECURITY AUDIT OF

HOLDSTATION MOBILE WALLET

Public Report

Oct 21, 2022

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
NFT	A non-fungible token (NFT) is a unique digital identifier that cannot be copied, substituted, or subdivided, that is recorded in a blockchain, and that is used to certify authenticity and ownership.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Oct 21, 2022. We would like to thank Holdstation for trusting Verichains Lab in auditing the mobile wallet. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the Holdstation Mobile Wallet. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified some vulnerable issues in the application, along with some recommendations.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Holdstation Mobile Wallet

Holdstation Mobile Wallet is a highly protected mobile app for your own decentralized experience.

1.2. Audit scope

In this particular project, a timebox approach was used to define the consulting effort. This means that **Verichains Lab** allotted a prearranged amount of time to identify and document vulnerabilities. Because of this, there is no guarantee that the project has discovered all possible vulnerabilities and risks.

Furthermore, the security check is only an immediate evaluation of the situation at the time the check was performed. An evaluation of future security levels or possible future risks or vulnerabilities may not be derived from it.

The security check was conducted on commit `eb89bd2111e8431df5ad24c559c9fbdf9a5d148a` from git repository *https://gitlab.com/hspublic/holdstation-mobile*.

1.3. Audit methodology

Verichains Lab's audit team mainly used the **Open Web Application Security Project (OWASP) Mobile Security Testing Guide (MTSG)**. The **MSTG** is a comprehensive manual for mobile app security development, testing and reverse engineering. It describes technical processes for verifying the controls listed in the **OWASP Mobile Application Verification Standard (MASVS)**. During the audit process, the audit team also used several tools for viewing, finding and verifying security issues of the app, such as following:

#	Name	Version
1	Mobile Security Framework (MobSF)	v3.5.0 beta
2	Frida tools	14.2.13
3	Android Studio	Bumblebee 2021.1.1
4	Visual Studio Code	1.64.2
5	Android Debug Bridge (adb)	1.0.41

Table 1. Tools used for audit

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the application functioning; creates a critical risk to the application; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the application with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the application with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 2. Severity levels

1.4. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure application. However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

The Holdstation Mobile Wallet was written in `JavaScript` Programming Language using `React Native` Framework. The source code is based on MetaMask Mobile wallet.

The main features of the Holdstation Mobile Wallet are:

- Manage multi-wallets under one account.
- Store, send and swap tokens.
- Import & Send NFT instantly.

2.2. Findings

During the audit process, the audit team found no vulnerability issue in the given version of Holdstation Mobile Wallet.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Oct 21, 2022*	Public Report	Verichains Lab

Table 3. Report versions history