Security Audit Report

04/28/2022

SafeSwap

Public Report

Summary

This report has been prepared for **SafeTech** and presents a summary of the results of the security audit completed on the **SafeSwap** project. It is based on the technical report which contains all the details and technical descriptions of the security assessment carried out by Red4Sec Cybersecurity.

The analysis shows that the project contained critical and high-risk vulnerabilities. However, the **SafeSwap** team has successfully and promptly fixed them.

Scope

Red4Sec Cybersecurity has made a thorough audit of the **SafeSwap** security level against attacks, identifying possible errors in the design, configuration or programming; therefore, guaranteeing the availability, integrity and confidentiality of the project and the possible assets treated and stored.

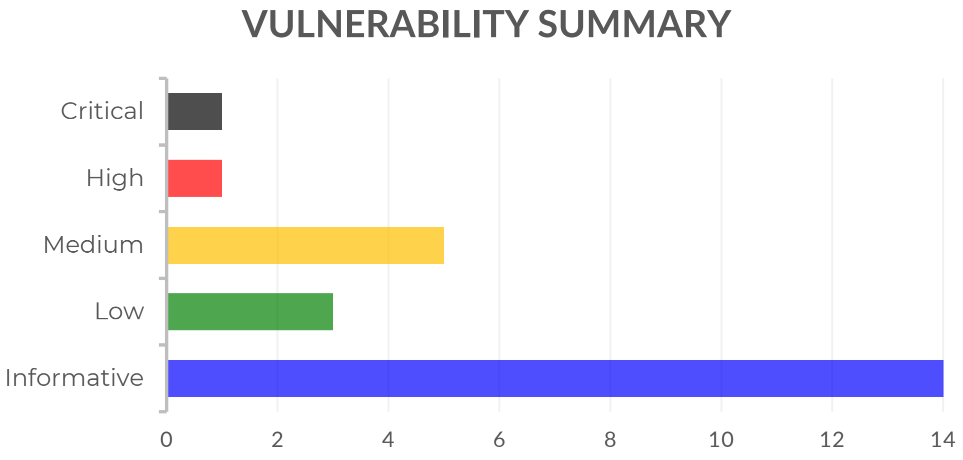
The scope of this evaluation includes the following projects enclosed in the main branch of https://github.com/SAFETECHio/SafeSwap-V1_red4sec repository, from commit `cdf3ba078f897161fc9fda662aee2876708f4c34` and the subsequent revision up to commit `c5d27fd236a1f07d472aa9272fd1052ee7480bb7`.

- `HashedTimelockERC20 Smart Contract`
- `API`
- `Swapper`

Executive Summary

The security audit against **SafeSwap** has been conducted between the following dates: **02/08/2022** and **02/22/2022**.

During the security assessment, a total of **24 vulnerabilities** were detected and classified by their risk level



Conclusions

To this date, **28th of April 2022**, the general conclusion resulting from the conducted audit of the projects specified on the scope, is that the **SafeSwap backend is secure** and does not currently present known vulnerabilities that could compromise the security of the users and their information.

A few of these vulnerabilities have already been solved by the **SafeSwap** team, thus helping to improve the security of the application.

The general conclusions of the performed audit are:

- Critical and High-risk vulnerabilities were detected during the security audit. All these vulnerabilities have been fixed by the **SafeSwap** team and subsequently reviewed and verified by the Red4Sec team.
- A few of the detected vulnerabilities do not pose a risk by themselves and have been classified as informative or low risk vulnerabilities. However, it is advisable to apply all the proposed recommendations in order to improve the project's source code and ecosystem, in fact, some of them were already fixed by the **SafeSwap** team.
- There was an on-chain verification of the data received and inserted in the API missing, this lack of verification could trigger denial of service.

Regarding the resilience of the system, it should be noted that, although the analyzed project adequately fulfils the desired functionality in relation to the code, it is necessary to accompany the project administration with external tools and procedures to guarantee the total confidentiality, integrity and availability of the bridge.

A few of the highlights that the **SafeSwap** team should pay special attention to are as follows:

- Include a complete monitoring and alert system of the smart contracts, API and backend services, in order to detect any failure in regard to the application, in funds of the bridge and/or in the swaps of the users.
- Perform an adequate separation of the privileges, both regarding the roles in the database, and of the systems in which the different components run, keeping the API isolated from the most critical components of the project, such as the swap and the database.
- The availability and integrity of the external RPC endpoints is critical and should be properly designed and dimensioned to avoid swap losses or malicious operations.
- The systems must have a properly configured time synchronization to avoid discrepancies between the systems and the different blockchains.

List of Vulnerabilities

In this section, you can find a complete list of the vulnerabilities detected in the security audit with their current status as of 04/28/2022.

Table of vulnerabilities			
ID	Vulnerability	Risk	State
HashedTimelockERC20 Smart Contract Issues			
STHT-01	Incompatible with Non-standard Tokens	**Informative**	**Assumed**
STHT-02	Outdated Compiler	**Informative**	**Fixed**
STHT-03	Outdated Third-Party Libraries	**Informative**	**Closed**
STHT-04	GAS Optimization	**Informative**	**Partially Fixed**
Docker Issues			
STDK-01	Lack of Environment Variables	**Informative**	**Fixed**
Database Issues			
STDB-01	Privilege Separation	**Medium**	**Open**
STDB-02	Wrong Types	**Medium**	**Fixed**
STDB-03	Database Design	**Informative**	**Assumed**
STDB-04	Database Exposed to Internet	**Informative**	**Assumed**
API Issues			
STAP-01	Lack of Rate Limit Controls	**High**	**Fixed**
STAP-02	Lack of Input Verifications	**Medium**	**Fixed**
STAP-03	Log Injection	**Medium**	**Assumed**
STAP-04	Wrong XSS Security Headers	**Low**	**Fixed**
STAP-05	Insufficient Control of Exceptions	**Low**	**Fixed**
STAP-06	HTML Injection	**Informative**	**Fixed**
STAP-07	Lack of HTTPS	**Informative**	**Assumed**
Swaper Issues			
STSW-01	New Swaps Denial of Service	**Critical**	**Fixed**
STSW-02	Apply Swaps Selection Criteria	**Low**	**Fixed**
STSW-03	Open ToDos	**Informative**	**Fixed**
STSW-04	Developer Information Leak	**Informative**	**Fixed**
STSW-05	Hardcoded API Key	**Informative**	**Assumed**
STSW-06	Third-Party Trust Delegation	**Informative**	**Assumed**

STSW-07	Outdated Packages	**Informative**	**Partially Fixed**
STSW-08	Possible XSS on email notifications	**Medium**	**Open**

Disclaimer

This document only represents the summarized results of the security assessment conducted by Red4Sec Cybersecurity and should not be used in any way to make investment decisions or as investment advice on a project.

Likewise, the report should not be considered neither "endorsement" nor "disapproval" of the guarantee of the correct business model of the analyzed project, nor as guarantee on the operation or viability of the implemented financial product.

Red4Sec makes full effort and applies every resource available for each audit, however it does not warrant the function, nor the safety of the project and it cannot be deemed a sufficient assessment of the project's utility and safety, bug-free status, or any other declarations of the project. Additionally, Red4Sec makes no security assessments or judgments about the underlying business strategy, or the individuals involved in the project.

RED4SEC

Invest in Security, invest in your future