Statement of work

Stronghold

IOTA Foundation

2022-05-04

Table of Contents

1 Introduction

The purpose of this document is to provide a statement of work performed by WithSecure during an assessment of the Stronghold secret management engine for the IOTA Foundation.

The results of the assessment are to be considered in the context of effort, time and budget spent, and within the context of the threat model and constraints in use during the assessment. Additionally, the listed results apply as a snapshot in time against a particular version of the audited code base, future code changes might introduce vulnerabilities not covered under this assessment. As such, it is possible that certain vulnerabilities have not been identified during the time allocated for the project.

This document does not serve as a certification of the results or the security of the application, and solely as a statement that WithSecure has performed a certain amount of security assessment work for the IOTA Foundation

2 Scope

2.1 Target

The following table identifies the version of the audited codebase.

Target Identifier	Description and Characteristics	Component Version
Stronghold	Stronghold is a secret management engine.	Branch dev-refactor[1]

2.2 Assessment Approach

The assessment was conducted based on the parameters described below.

Location	Off-site
Effort	17 days source code review
Timespan	March 21, 2022 – April 4, 2022
Target Lifecycle State	Development
Attacker View	Anonymous and trusted user (unauthenticated and authenticated as regular user)
Methodology	White-box, WithSecure had full insight into all details regarding the target(s) such as source code, etc

2.3 Assessment Constraints

The audit has been conducted under the following assumptions:

- Adversary has not compromised the underlying operating system
- Adversary has the same level of privileges as the one using the wallet
- Adversary is not root or does not have administrator rights on the system
- Adversary has not instrumented or modified the binary

Attack scenarios depending on any of the conditions listed above, or a combination of them, have not been covered by this audit.

[1] The branch was at commit eb07c4a4

3 Summary of Results

The purpose of this security assessment was to analyze the Stronghold secret management engine developed by the IOTA Foundation and attempt to use it in a way not specified during the design process. The project focused on identifying security vulnerabilities with the goal of establishing the current security level of the audited application.

This report is meant as a statement that this application underwent an assessment by WithSecure and only provides a summary overview of the findings made during the assessment and does not describe full technical details.

As several constraints affected the assessment, directly influencing the results and achieved coverage, WithSecure recommends readers of this report to take the constraints, described in the Assessment Constraints section, into account to ensure a proper understanding of the findings within their context and the overall security level.

3.1 Summary of Vulnerabilities

The following table presents all the issues that were identified, ordered by severity and prevalence and their status after the verification test conducted to verify the mitigations deployed by the IOTA Foundation.

Target	Vulnerability Description
Stronghold	Insufficient zeroization of sensitive data
Stronghold	p2p protocol not protected against replay attacks
Stronghold	Outdated third-party dependency
Stronghold	Unsafe Key derivation function[2]
Stronghold	Memory allocation schema in memory protection deviates from best practices
Stronghold	Potentially unsafe hashing function in memory protection

[2] This finding has been marked invalid as the Customer confirmed that the affected function is former code still present in the codebase but not actually used in latest stronghold releases.