VULNERABILITY ASSESSMENT

Ravencoin

EXECUTIVE SUMMARY

Overview

Ravencoin engaged Independent Security Evaluators (ISE) to evaluate the security posture of the Ravencoin project, an open-source peer-to-peer blockchain used to enable transactions between users, with a specific focus on asset creation and transfer functionality. ISE performed an assessment to discover vulnerabilities within the system that could lead to the compromise of the Ravencoin asset layer, the integrity of user assets, or the availability of the service.

ISE considers attack surfaces, permissions, and application logic specific to Ravencoin that an advanced attacker may exploit, and manually tests against such exploits. ISE uses automated tools to gain an understanding of the system and identify common issues, but the focus of the assessment is discovering vulnerabilities that scanners will miss. ISE reviews all reported findings for accuracy and assigns severity based on exploit complexity, impact, and attack chaining.

ISE has assessed the following components:

- Asset Creation Functionality
- Asset Transfer Functionality
- Asset Related RPCs
- Source Code Review
- Review of KAWPOW
- Review of Distributable Binaries

While the focus of this assessment was on asset creation and transfer functionality, implementation of KAWPOW, and messaging, ISE did not uncover any security defects that would allow for unintended asset creation, asset transfer, or denial of service within the system

Scope

As of this report, ISE has assessed the following components:

- Ravend, Raven-qt, version 4.3.2.1
- Ravencoin specific RPCs

Methodology

ISE specializes in hands-on assessments that consider assets, attack surfaces, permissions, and logic specific to the target system. The goal is to discover security issues that a variety of attackers may exploit, and manually test against such exploits using access to the platform, e.g., test accounts, server access, source code, documentation, etc. In general, ISE encourages sharing as much relevant access as possible because a deeper knowledge of the system facilitates more efficient testing and more valuable results.

ISE performed the assessment of Ravencoin with access to the following resources:

- Source code located at https://github.com/RavenProject/Ravencoin/tree/v4.3.2
- Documentation and build instructions

ISE used automated tools to gain an understanding of the system and identify common issues, but the focus of the assessment was discovering vulnerabilities that scanners will typically miss. ISE reviews all reported findings for accuracy and assigns severity based on exploit complexity, impact, and attack chaining.

Below is a list of core areas of testing, including but not limited to:

Ravencoin/Bitcoin Code Delta:

ISE conducted a review of code changes integrated since the Bitcoin 0.15.x code fork for security defects that may affect the usability, stability, or security guarantees provided by Ravencoin. This review was meant to familiarize ISE with Ravencoin implementation details as well as the identification of functionality that may be considered a security defect. This review consisted of a diff based analysis approach (to eliminate Bitcoin core code, which was out of scope for this engagement), along with static code review, and dynamic runtime testing. Results of these tests resulted in the identification of 'ISE-RAVEN-2020-02'. Additional tests were performed on frameworks or libraries used. Results of these tests resulted in the identification of 'ISE-RAVEN-2020-01' and 'ISE-RAVEN-2020-03'.

Ravencoin Asset Layer:

ISE conducted a review of Ravencoin Asset creation, reissue, messaging, and transfer workflows. The bulk of ISE resources was dedicated to this area. Review of the asset layer was done by performing a source code review, dynamic analysis/fuzzing of functionality, and evaluation of associated script code. Asset related RPCs and code paths were also reviewed to ensure implied security guarantees could not be violated. That is, asset workflows should not lead to the unauthorized generation of Ravencoin itself, nor should asset quantities be modified in an unintended way. The results of analysis in this area were negative. ISE did not find any functionality that could be used in unintended ways to bypass or exploit the creation, reissue, and transfer of assets. Nor could assets, or messaging be used to create an application layer of denial-of-service scenario through exploitation of application layer asset related code.

Ravencoin Consensus:

ISE performed a review of Ravencoin's implementation of a modified ProgPoW, created to help prevent centralization, adopted as KAWPOW. This entailed a code review of Ravencoin specific changes, and tuning parameters. ISE noted no implementation defects in KAWPOW.

Ravencoin Binaries:

ISE reviewed Ravencoin's installation workflows and binaries to identify items that would reduce the security of the distribution channel, or lack of mitigation protections against runtime exploits. Results of these tests resulted in 'ISE-RAVEN-2020-04' and 'ISE-RAVEN-2020-05'.

Timeline

A history of ISE's assessments is shown in the table below.

Revision	Date	Description
1	Nov – Dec 2020	Initial assessment of Ravencoin.

This report expires on December 31, 2021. Expiration facilitates ongoing communication and assessment efforts to address changes in technology, the product, and its supporting environment.

Findings Summary

The following tables contain the vulnerabilities and strategic weaknesses ISE has identified in the Ravencoin platform. Each issue is assigned a severity that is derived from the issue's impact to Ravencoin's assets and its exploitability.

Vulnerabilities

Vulnerabilities are directly exploitable in some manner, and ISE's analysis considers the complexity of performing a given exploit, along with the impact if an attack were successful.

RAVENCOIN CORE COMPONENTS

Vulnerability	Identifier	Severity	Status
Use of Out-of-Date Bitcoin Fork	ISE-RAVEN-2020-01	Low	Unresolved
Faulty Conditional Logic	ISE-RAVEN-2020-02	Info	Unresolved

Strategic Weaknesses

Strategic weaknesses may not be directly exploitable but are design or configuration related issues that may lead to security problems over time while maintaining a product's codebase.

RAVENCOIN CORE COMPONENTS

Weakness	Identifier	Severity	Status
Use of Out-of-Date Qt Framework	ISE-RAVEN-2020-03	Low	Unresolved
Windows Signed Installer uses Untrusted Certificate	ISE-RAVEN-2020-04	Low	Unresolved
Lack of Signed Binaries	ISE-RAVEN-2020-05	Info	Unresolved

About ISE

ISE is an independent security firm headquartered in Baltimore, Maryland. We are dedicated to providing clients proven scientific strategies for defense. On every assessment our team of analysts and developers use adversary-centric approaches to protect digital assets, harden existing technologies, secure infrastructures, and work with development teams to improve our clients' overall security.

Assessing the client through the eyes of potential attackers allows us to understand possible threats and how to protect against those attacks. Our security analysts are experienced in information technology and product development which allows them to understand the security problems the client faces at every level. In addition, we conduct independent security research which allows us to stay at the forefront of the ever-changing world of information security.

Attacks on information systems cannot be stopped, however with robust security services provided by an experienced team, the effects of these attacks can often be mitigated or even prevented. We appreciate the confidence placed in us as a trusted security advisor. Please don't hesitate to get in touch for additional assistance with your security needs.

Independent Security Evaluators, LLC

4901 Springarden Drive
Suite 200
Baltimore, MD 21209
(443) 270-2296

contact@ise.io

https://www.ise.io