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.

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 and other resources.

ISE reviews all reported findings for accuracy and assigns severity based on exploit complexity, impact, and attack chaining.

APPLICATION AND API TESTING

ISE assessed the Ravencoin platform by manually testing its functionality for vulnerabilities and developing custom exploits where applicable. ISE used automated tools to gain an understanding of the application and identify common issues, but the focus of the assessment was identifying issues that a scanner would miss. The following is a list of core areas of testing:

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

ACCESS

ISE performed the assessment with access to the following resources:

- Source code.
- Documentation and build instructions.

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