Factom® Protocol Bug Bounty Program

Overview

The Factom® Protocol Bug Bounty Program provides bounties for vulnerabilities and exploits discovered in the Factom® Protocol or any of the code in the Factom® Protocol source code repositories. We recognize the importance of our community and security researchers in helping identify bugs and issues. We encourage responsible disclosure of security vulnerabilities via our bug bounty program described on this page.

Responsible Disclosure

The Factom® Protocol core development team has up to 90 days to implement a fix based on the severity of the report. Please allow for this process to fully complete before you publicly disclose the vulnerability.

Rewards

We are rewarding researchers that find bugs with a bounty in our digital currency, factoids (FCT). The amount of the award depends on the severity of the vulnerability reported. The Factom® Protocol Core Committee will evaluate the award according to the severity calculated according to the OWASP risk rating model based on Impact and Likelihood. However, final awards are determined at the sole discretion of the committee:

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

- Critical: up to 2500 points
- High: up to 1500 points
- Medium: up to 500 points
- Low: up to 200 points

- Note: up to 50 points

1 point currently corresponds to 1 USD, payable in Factoids (FCT), something which may change without prior notice.
Researchers are more likely to earn a larger reward by demonstrating how a vulnerability can be exploited to maximum effect.

Eligibility

Generally speaking, any bug that poses a significant vulnerability to the security or integrity of the Factom® Protocol Network could be eligible for reward. However, it's entirely at our discretion to decide whether a bug is significant enough to be eligible for reward.
In general, anything which has the potential for financial loss or a breach of data is of sufficient severity, including:

- Implementation bugs that can lead to financial loss
- Access to authority set nodes
- Remote Code Execution
- Protocol bugs
- Node crash bugs in the core Factom® Protocol (ex. a bug that can crash the node by sending a special request, not by sending thousands requests).

In general, the following would not meet the threshold for severity:

- Recently disclosed 0-day vulnerabilities
- Vulnerabilities on sites hosted by third parties unless they lead to a vulnerability on the Factom® Protocol website https://factomprotocol.org.
- Vulnerabilities contingent on physical attack, social engineering, spamming, DDOS attack, etc.
- Vulnerabilities affecting outdated or unpatched software.
- Vulnerabilities in third party applications that make use of Factom® Protocol's APIs.
- Bugs that have not been responsibly investigated and reported.
- Bugs already known to us, or already reported by someone else (reward goes to first reporter).
- Vulnerabilities that have been disclosed to the public
- Issues that aren't reproducible.
- Issues that we can't reasonably be expected to do anything about.
- Anyone that works with the codebase as a professional Factom core developer

Severity

The severity of a bug, i.e. how many participants in the Factom® Protocol network are affected, is taken into consideration when deciding the bounty payout amount. For example,

an exploit that relies on an implementation bug in the Factom® Protocol affects the network as a whole and very deeply. As there are currently no alternate implementations of the Factom® Protocol node software (factomd) it means that bug bounty payout that affects the Factom® Protocol nodes would be higher than for example, a client library bug.

Scope

Open source projects:

- Factomd (node)
- Walletd (wallet software)
- Enterprise wallet
- Factom-cli (CLI)

Clients:

- Javascript client
- Java & Android client
- Python client
- C#/.Net client

Websites:

- https://factomprotocol.org
- https://factomize.com/forums
- https://factomd.net

Other services that, when exploited, lead to security bugs in above.

Best practices

Please use a local network (https://developers.factomprotocol.org/start/developer-sandbox-setup-guide) and not the test/public network when searching for security bugs. Remember that blockchains are public and someone may see your findings and report a bug before you and a successful attack might impact others, even when testing the attack vector(s).

A step by step report (or an exploit script) is very much welcome. It will allow us to understand and fix the issue faster and you will get your rewards more quickly.

Report a bug

- Create a new thread on the Factomize forum https://factomize.com/forums/factom/bug-bounty/. Only you and the core committee can see the thread.
- Try to include as much information in your report as you can, including a description of the bug, its potential impact, and steps for reproducing it or proof of concept.
- Include your Factoid (FCT) address for payment.
- Please allow 3 business days for the core committee to respond in the forum thread before reminding them.

Legal

You may not participate in this program if you are a resident or individual located within a country appearing on any U.S. sanctions lists.