CERTIK

Injective Protocol

Security Assessment

September 20th, 2020

For :
Eric @ Injective Protocol
Eric@InjectiveProtocol.com

By :
Angelos Apostolidis @ CertiK
angelos.apostolidis@certik.org

Disclaimer

CertiK reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts CertiK to perform a security review.

CertiK Reports do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

CertiK Reports should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

CertiK Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

What is a CertiK report?

- A document describing in detail an in depth analysis of a particular piece(s) of source code provided to CertiK by a Client.
- An organized collection of testing results, analysis and inferences made about the structure, implementation and overall best practices of a particular piece of source code.
- Representation that a Client of CertiK has indeed completed a round of auditing with the intention to increase the quality of the company/product's IT infrastructure and or source code.

What isn’t a CertiK report?

- A statement about the overall bug free or vulnerability free nature of a piece of source code or any modules, technologies or code it interacts with.
- Guarantee or warranty of any sort regarding the intended functionality or security of any or all technology referenced in the report.
- An endorsement or disapproval of any company, team or technology.

Summaries

Project Summary

Project Name	Injective Protocol
Description	ERC-20 Token
Platform	Ethereum, Solidity
Commit Hash	aa44945b47685ab986bbb21f89120b115f50efd6

Audit Summary

Delivery Date	Sep. 20, 2020
Method of Audit	Static Analysis, Manual Review
Consultants Engaged	1
Timeline	Sep. 19th, 2020 - Sep. 20th 2020

Vulnerability Summary

Total Issues	1
Total Critical	0
Total Major	0
Total Minor	0
Total Informational	1

Findings

ID	Title	Type	Severity
IP-01	Potential Race Condition	Volatile Code	Informational

IP-01: Potential Race Condition

Type	Severity	Location
Volatile Code	Informational	InjectiveToken.sol: Line 7

Description:

The ERC-20 standard inherently possesses a race condition whereby a set amount is approved and the user subsequently decides to update this approval to an increased amount. In the window the transaction that increases the approval is broadcasted, an attacker would be able to fully utilize any remaining allowance as well as the newly set one, thus leading to a type of "double" approval attack.

Recommendation:

This can be mitigated by first ensuring approval has been set to zero before being increased to some other value. Other workarounds also exist and would preferably be applied in this case.