World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:17, No:01, 2023

Static Application Security Testing Approach for Non-Standard Smart Contracts

Authors : Antonio Horta, Renato Marinho, Raimir Holanda

Abstract : Considered as an evolution of the Blockchain, the Ethereum platform, besides allowing transactions of its cryptocurrency named Ether, it allows the programming of decentralised applications (DApps) and smart contracts. However, this functionality into blockchains has raised other types of threats, and the exploitation of smart contracts vulnerabilities has taken companies to experience big losses. This research intends to figure out the number of contracts that are under risk of being drained. Through a deep investigation, more than two hundred thousand smart contracts currently available in the Ethereum platform were scanned and estimated how much money is at risk. The experiment was based in a query run on Google Big Query in July 2022 and returned 50,707,133 contracts published on the Ethereum platform. After applying the filtering criteria, the experimentgot 430,584 smart contracts to download and analyse. The filtering criteria consisted of filtering out: ERC20 and ERC721 contracts, contracts without transactions, and contracts without balance. From this amount of 430,584 smart contracts selected, only 268,103 had source codes published on Etherscan, however, we discovered, using a hashing process, that there were contracts duplication. Removing the duplicated contracts, the process ended up with 20,417 source codes, which were analysed using the open source SAST tool smartbugswith oyente and securify algorithms. In the end, there was nearly $100,000 at risk of being drained from the potentially vulnerable smart contracts. It is important to note that the tools used in this study may generate false positives, which may interfere with the number of vulnerable contracts. To address this point, our next step in this research is to develop an application to test the contract in a parallel environment to verify the vulnerability. Finally, this study aims to alert users and companies about the risk on not properly creating and analysing their smart contracts before publishing them into the platform. As any other application, smart contracts are at risk of having vulnerabilities which, in this case, may result in direct financial losses.

Keywords : blockchain, reentrancy, static application security testing, smart contracts
Conference Title : ICCSA 2023 : International Conference on Cybersecurity and Security Analysis
Conference Location : Amsterdam, Netherlands
Conference Dates : January 23-24, 2023