Compound Deployment Validation

In addition to audits, we offer deployment validation for audited code. Deployment Validation Files (DVF) is a tool designed to ensure that smart contracts are deployed with the expected bytecode and configuration. Trusted entities can sign and publish DVFs, which can then be checked against on-chain smart contracts to verify correct deployment at any specified block number. Each DVF describes the correct state of a single smart contract and may reference other DVFs for dependent contracts, enabling comprehensive validation.

This detects incidents where the wrong code version was deployed and detects accidental misconfigurations. It also detects attacks with maliciously backdoored contracts.

An example of accidental misconfiguration which could have been prevented by our deployment validation tool is Compound's proposal 226, which contained an incorrect parameter. This led to an unintended high borrowing APR for the Arbitrum USDC market.

It also covers contracts that were maliciously manipulated by insiders such as in the case of the $60m+ Munchables exploit. The exploit was made possible due to a malicious developer hiding large token allocations to themselves during deployment. The verified code inspectable on block explorers made it look like this was impossible. The ERC20 standard makes it notoriously hard to list all balances of all users as it is only possible to query a user's balance if their address is known beforehand. Our deployment validation tool not only ensures that the code is as intended, but also that all the state is as expected. It detects these cases where e.g. a hidden token balance is present, or where hidden admin accounts have been set up.

Github link: https://github.com/chainsecurity/deployment_validation