Dedaub

Security Technology for Smart Contracts

YesBit ERC 721 NFT Contract (ERC721SWAPO)

Date: Nov. 27 2020

Dedaub was commissioned to perform a security audit on the SWAPO token, currently deployed to the Ethereum mainnet at address `0xD338594c13Fa239Fba0dE80230Ca03bD729439cD`. The contract implements a non-fungible token, per the ERC 721 standard.

The token is fully implemented based on recent versions of the standard OpenZeppelin libraries, so it should be considered secure.

In particular, the main part of the contract is derived from OpenZeppelin's ERC721.sol (and the sources it includes), updated at some point after commit `ca7ee09`, i.e., within the last two months. There is no newer update to these OpenZeppelin libraries that seems to affect the contract's functionality, with the minor exception of newer code supporting higher Solidity compiler versions.

There is a low risk of issues given that these libraries have been reused in several other projects. Nevertheless, we also performed thorough code inspection independently of the provenance of the code, as if it had been written from scratch. We also decompiled the code and analyzed it thoroughly, using our static analysis (incl. symbolic execution) tools, to detect possible issues. This report is a revised version, after implementation of our original audit suggestions which are fully addressed.

Trust Model

[*This section is included for context, although its contents should already be known to the commissioner of an audit.*]

Users of the token need to be comfortable with several centralization elements:

- Minting and burning of the token is performed by a single ERC721SWAPO administrator/owner. This owner is not to be confused with the owner of individual non-fungible tokens.
- The ERC721SWAPO owner can burn any holder's tokens at any time. As a consequence, the ERC721SWAPO owner can replace the owner of any token, by burning it and re-minting it. Additionally, the ERC721SWAPO owner can change any URIs associated with individual tokens (or the URI base). In short, all owners of tokens have to fully trust the ERC721SWAPO owner.

- The current owner of an individual token cannot change any aspect of the token, or burn it. Individual tokens are immutable (except to the globally-trusted ERC721SWAPO owner).

Critical Severity

No critical severity vulnerabilities were identified

High Severity

No high severity vulnerabilities were identified

Medium Severity

No medium severity vulnerabilities were identified

Low Severity

No low severity vulnerabilities were identified

Lowest/Code/Style/Info/Suggestions

Generally, we recommend a practice of local testing followed by a testnet deployment, instead of deploying to the mainnet. We understand that the current deployment was done with the confidence that this is a composition of trusted OpenZeppelin components, but even a simple composition could contain mistakes.

The contract was compiled with the Solidity compiler `v0.6.12` which has some known minor issues (but relatively few, compared to earlier versions). We have reviewed the issues and do not believe them to affect the contract. The main concern might have been issue `EmptyByteArrayCopy`, identified recently. The contract is not affected: the issue requires copying zero-length memory arrays to storage, and the contract only does this for public calls (`setBaseURI`, `setTokenURI`) from the trusted ERC721SWAPO owner account.

Disclaimer

The audited contracts have been analyzed using automated techniques and extensive human inspection in accordance with state-of-the-art practices as of the date of this report. The audit

makes no statements or warranties on the security of the code. On its own, it cannot be considered a sufficient assessment of the correctness status of the contract. While we have conducted an analysis to the best of our ability, it is our recommendation for high-value contracts to commission several independent audits, as well as a public bug bounty program.

About Dedaub

Dedaub offers technology and auditing services for smart contract security. The founders, Neville Grech and Yannis Smaragdakis, are top researchers in program analysis. Dedaub's smart contract technology is demonstrated in the contract-library.com service, which decompiles and performs security analyses on the full Ethereum blockchain.