



Security Audit Report

ExampleToken (EXT)

This is an illustrative sample. The project, address and findings are fictional and show the structure of a delivered report.

NETWORK

BNB Smart Chain (BEP-20)

LANGUAGE

Solidity ^0.8.20

METHODS

Manual review · Static analysis · Unit tests

CONTRACT ADDRESS

0x00000000000000000000000000000000000000000000000000000000000000E5T

AUDIT DATE

October 2026

RESULT

PASSED — score 82 / 100

Executive summary



Findings by severity



The contract implements a BEP-20 token with transfer fees, an owner-controlled fee setter and a staking vault. No critical issues were found. One high-severity reentrancy issue in the vault was fixed by the team during the audit; the remaining medium issues are centralisation risks that the team acknowledged.

Findings overview

ID	TITLE	SEVERITY	STATUS
EXT-01	Reentrancy in withdraw()	HIGH	Fixed
EXT-02	Owner can change fees without a cap	MEDIUM	Acknowledged
EXT-03	No timelock on privileged functions	MEDIUM	Acknowledged
EXT-04	Missing events for parameter changes	LOW	Fixed
EXT-05	Unchecked return value of transfer	LOW	Fixed
EXT-06	Floating pragma	LOW	Fixed
EXT-07–10	Gas optimisations and naming	INFO	Fixed

Detailed findings

HIGH EXT-01 · Reentrancy in withdraw()

The vault sends tokens to the caller before updating their balance, so a malicious token hook can re-enter withdraw() and drain funds.

```
function withdraw(uint256 amount) external {
  require(balances[msg.sender] >= amount);
  token.transfer(msg.sender, amount); // external call first
  balances[msg.sender] -= amount;    // state updated after
}
```

Recommendation: update state before the external call (checks-effects-interactions) and add a nonReentrant guard. **Fixed in commit a1b2c3d.**

MEDIUM EXT-02 · Owner can change fees without a cap

setFee() accepts any value up to 100%, so the owner could block transfers. **Recommendation:** cap fees (e.g. $\leq 10\%$) and emit an event. **Acknowledged.**

MEDIUM EXT-03 · No timelock on privileged functions

Owner functions take effect immediately. **Recommendation:** move ownership to a multisig behind a 24–48 h timelock. **Acknowledged.**

Disclaimer

An audit reduces risk but cannot guarantee that a contract is free of vulnerabilities. This sample is for illustration only and does not describe a real project.