# Security Audit Complete

OTCSwap V4 — All Critical Issues Resolved

We recently completed a focused security audit of the OTCSwap smart contract (the core escrow engine behind SwapNFT.xyz). Three critical vulnerabilities were identified in earlier versions. All three have been fully fixed in OTCSwap V4.

 Outcome: The protocol now enforces strict deposit validation, uses safe pull-based ETH handling, and rejects fake NFT offers. Your assets are protected by these hardened mechanisms.

Audit tooling: Paradigm EVM Bench

(Tooling credit only — not an endorsement)

## What Was Found & Fixed

1. ERC20 Deposit Validation
Fee-on-transfer tokens could cause under-collateralized orders and drain shared balances. Fixed: V4 now strictly verifies the exact amount received before accepting any deposit.

2. ETH Transfer Locking
ETH sent to non-payable contract addresses could become permanently stuck. Fixed: We moved to a pull-based withdrawal system so users can always claim their ETH safely.

3. Fake NFT Offers
Malicious makers could advertise non-existent NFTs and steal taker deposits. Fixed: Every NFT leg now requires a real contract + proof that the NFT was actually escrowed.

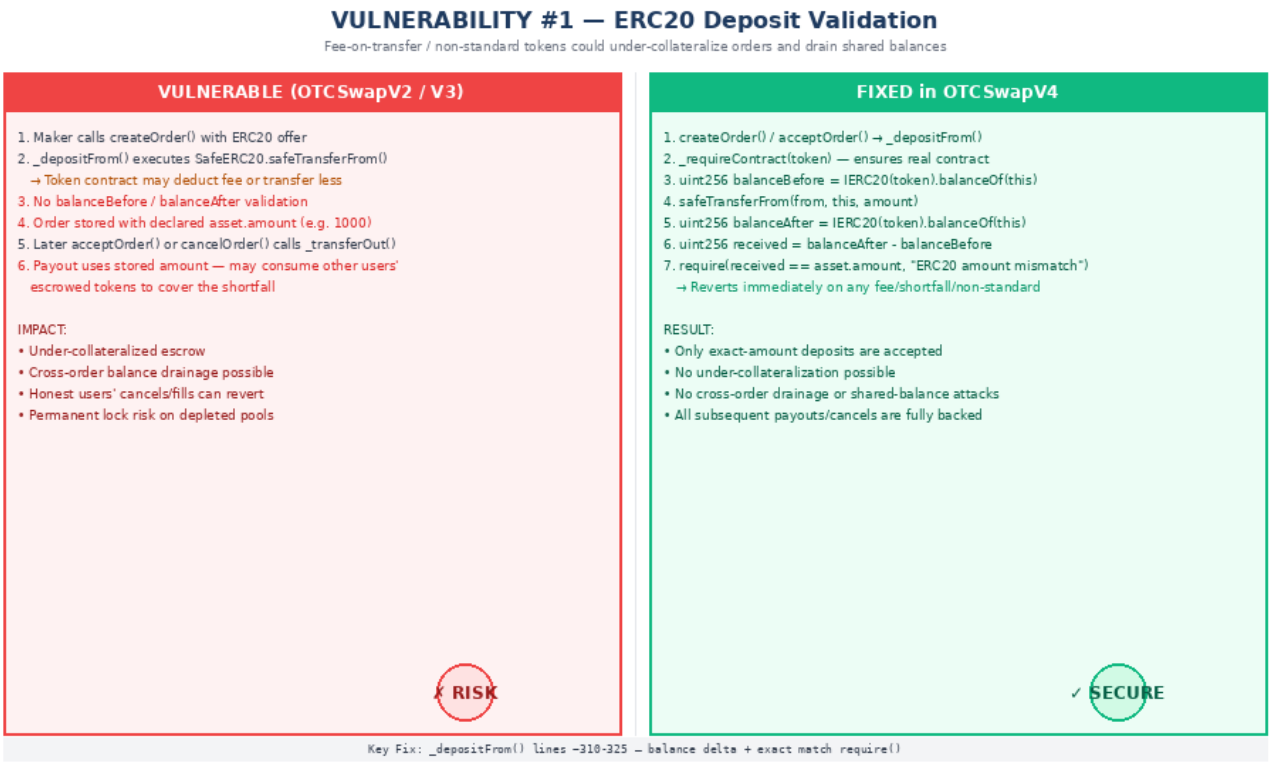
These fixes were implemented with minimal, targeted changes and follow industry best practices for escrow contracts. The V4 contract has been thoroughly reviewed against the original findings.

Full technical audit report (10 pages, with code snippets and detailed analysis) is available for developers and auditors. Download link at the bottom of this summary.

# How the Fixes Work (Visual Overview)

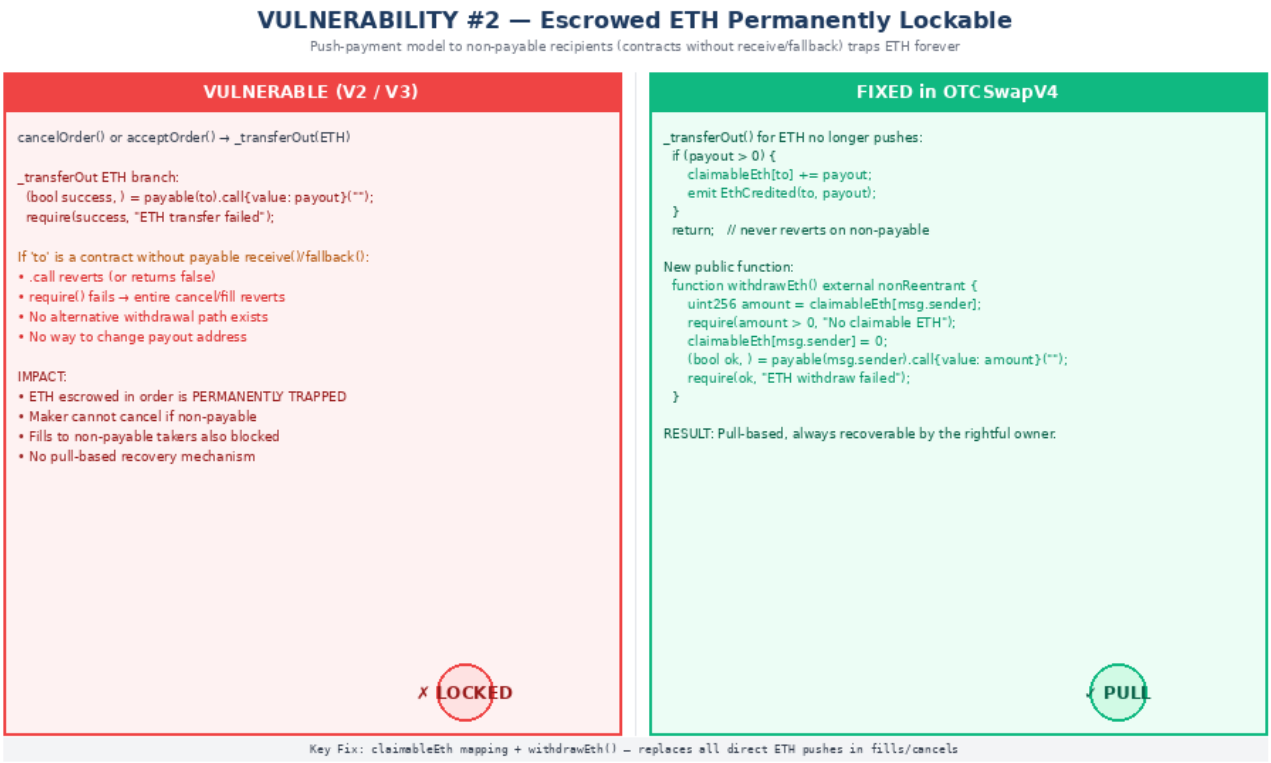
Below are simple before/after diagrams showing the problems we fixed and how OTCSwap V4 now protects users.

1. ERC20 Deposits — Preventing Under-Collateralization

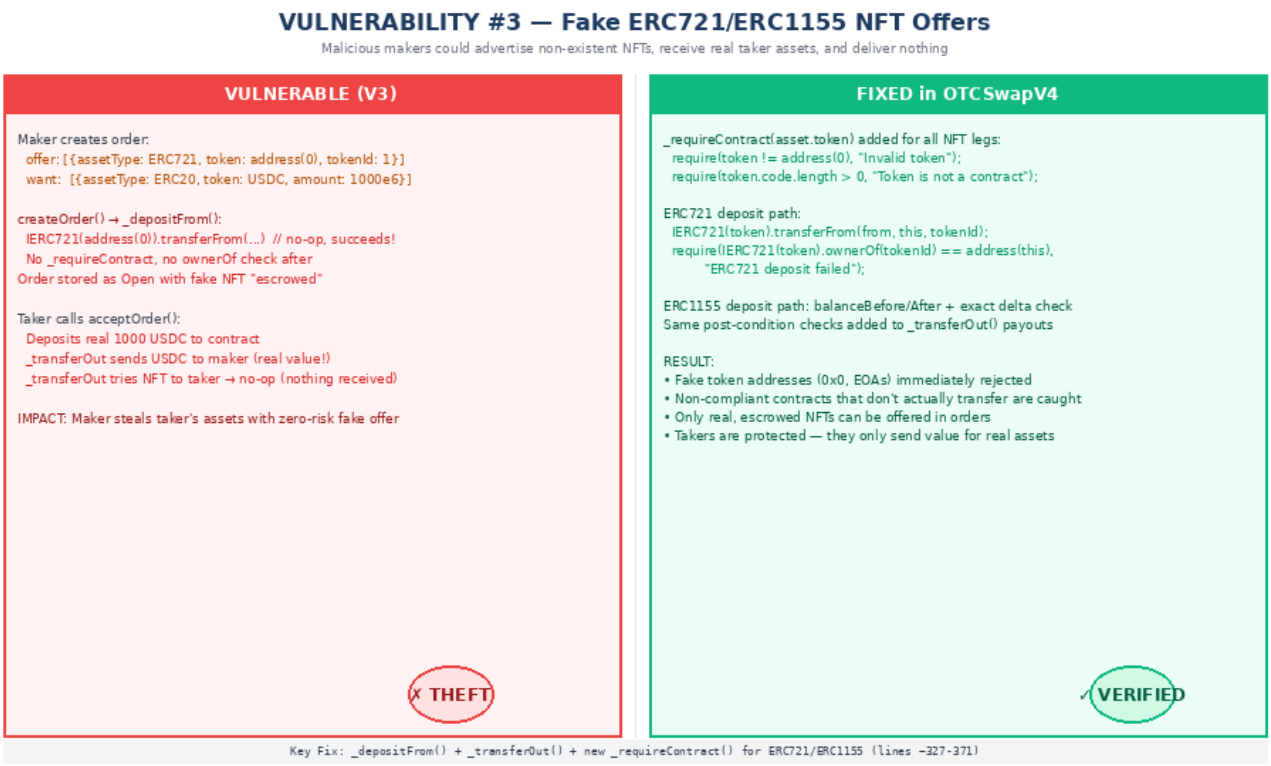



Result: Only orders backed by the exact declared amount of tokens are created. No more silent shortfalls or draining of other users' funds.

2. ETH Handling — No More Locked Funds




3. NFT Offers — Blocking Fake Assets




Your assets are now protected by these improvements.

OTCSwap V4 rejects unsafe deposits, prevents locked ETH, and only allows real escrowed NFTs to be traded. We take security seriously and will continue to monitor and improve the protocol.

## Download the Full Technical Report

For developers, auditors, or anyone who wants the complete details (including exact code changes and proof-of-concept analysis), you can download the full 10-page technical audit report here:

**Full Technical Audit Report (PDF)**
**OTCSwapV4_Security_Audit_Report.pdf — 10 pages with code-level details**

This public summary and the full technical report were prepared in July 2026. SwapNFT.xyz is committed to transparency and the ongoing security of user funds.