In June 2022, the XCarnival smart contract was exploited for approximately $3.8 million in tokens.  XCarnival is an NFT lending platform in which a user can deposit an NFT as collateral against loans.  The XCarnival hack [was made possible by an error](https://twitter.com/BenWAGMI/status/1541145543514411008) in how the smart contract tracked deposited collateral and a user’s eligibility for loans.

**INSIDE THE ATTACK**

When a user deposits NFTs into the platform, they are assigned an orderID that they can take out loans against.  In theory, this orderID would only be valid for as long as the NFT was deposited as collateral with the platform.  In practice, the smart contract kept the orderID open even after the collateral was withdrawn.

The XCarnival attacker took advantage of this to drain value from the project.  They created a smart contract with several child contracts.  In turn, each child contract deposited an NFT as collateral and borrowed nothing to get a valid orderID and then withdrew the collateral NFT and returned it to the parent contract for use by the next child contract.

Once all of the children had a valid orderID, the attacker called each in turn to borrow ETH.  Since the orderIDs were valid and hadn’t been revoked, the borrows succeeded, enabling the theft of ~$3.8 million in ETH.

**LESSONS LEARNED FROM THE ATTACK**

The XCarnival hack was made possible by an oversight in the management of orderIDs, which should have been revoked as soon as the collateral was removed.  A failure to do so allowed multiple loans to be made against the same NFT, which had already been withdrawn as collateral.

This sort of business logic error should have been identified within a smart contract audit.  If it had been, the project may have been saved a $3.8 million breach.