In September 2021, the Vee Finance protocol was the victim of a hack.  This DeFi project, based on the Avalanche Network, lost approximately $34 million in tokens to an attacker that exploited a pair of mistakes in the project’s smart contract.

**INSIDE THE ATTACK**

The Vee Finance hack was made possible by how the protocol handles slippage checks for leveraged trading.  The first mistake made by the protocol was [using only a single oracle](https://veefi.medium.com/the-main-cause-of-vee-finance-attack-7a8475085ec5) for determining the price of assets used in trading.

This is a common error that has been exploited in numerous DeFi hacks.  When a project relies on a single source of truth for price information, an attacker can manipulate pricing information.

In this case, the attacker [created several new trading pairs](https://www.rekt.news/veefinance-rekt/) on the exchange.  The attacker then performed trades between these newly-created pairs, causing their apparent prices on Pangolin (the only price oracle used by Vee Finance) to be distorted.  By manipulating token prices in Pangolin, the attacker was able to bypass the slippage checks on Vee Finance.  This issue was exacerbated by the fact that when calculating the amount of Token B that can be received in exchange for Token A the decimal values of the token prices are not included.

The combination of incorrect price information and errors in price calculation caused Vee Finance to approve transactions that should have been rejected.  As a result, the attacker was able to siphon approximately $34 million in tokens from the protocol.

**LESSONS LEARNED FROM THE HACK**

The Vee Finance hack was made possible by two common errors.  First, the protocol used only a single oracle for price information, a mistake that lies behind many [flashloan attacks](https://halborn.com/what-is-a-flash-loan-attack/).  Also, the price calculations used when evaluating trades included a fundamental mathematical error.

These issues should have been detected during a security audit, and, in fact, they likely were but were ignored.  An [audit by Slowmist raised multiple concerns](https://github.com/VeeFinance/audit/blob/main/2021-9-09_SlowMist%20Security%20Audit%20Vee%20Finance/Smart%20Contract%20Security%20Audit%20Report%20-%20Vee%20Finance.pdf) about the use of oracles by the protocol, which Vee Finance ignored.

Hacks like this demonstrate the importance not only of undergoing a security audit but also of listening to its results.  If audit results regarding oracles had not been ignored, then this hack may not have happened.