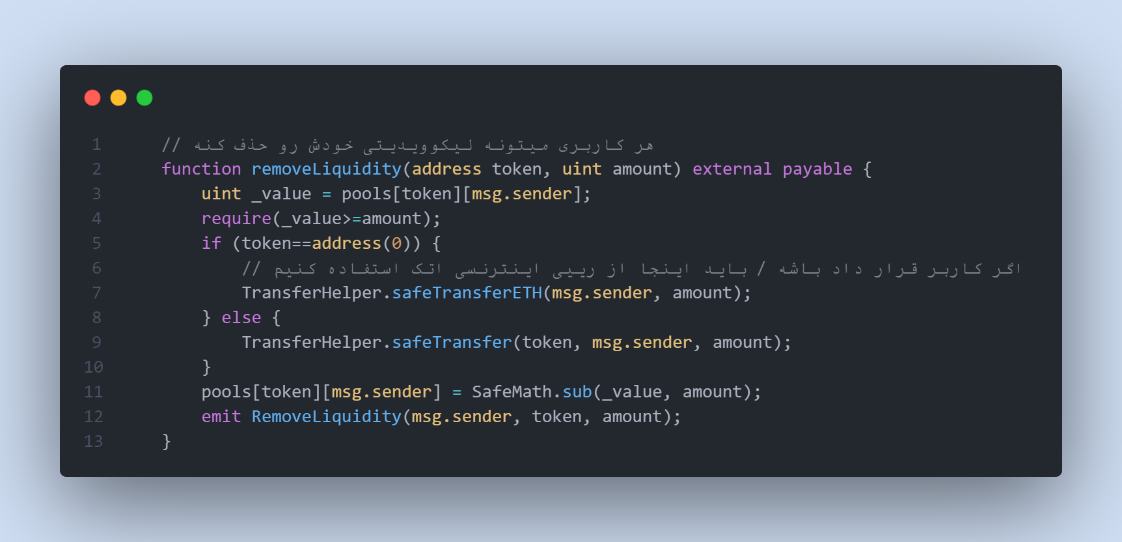
# **https://www.certik.com/projects/neonlink**

# **High severity issues**

* **Reentrancy Vulnerability Allows The Attacker To Drain All TheETH From The Contract.**

**The "removeLiquidity()" and “transfer” function transfers ETH to the user with an external call and updates the user'sbalance after the token transfer.**



****

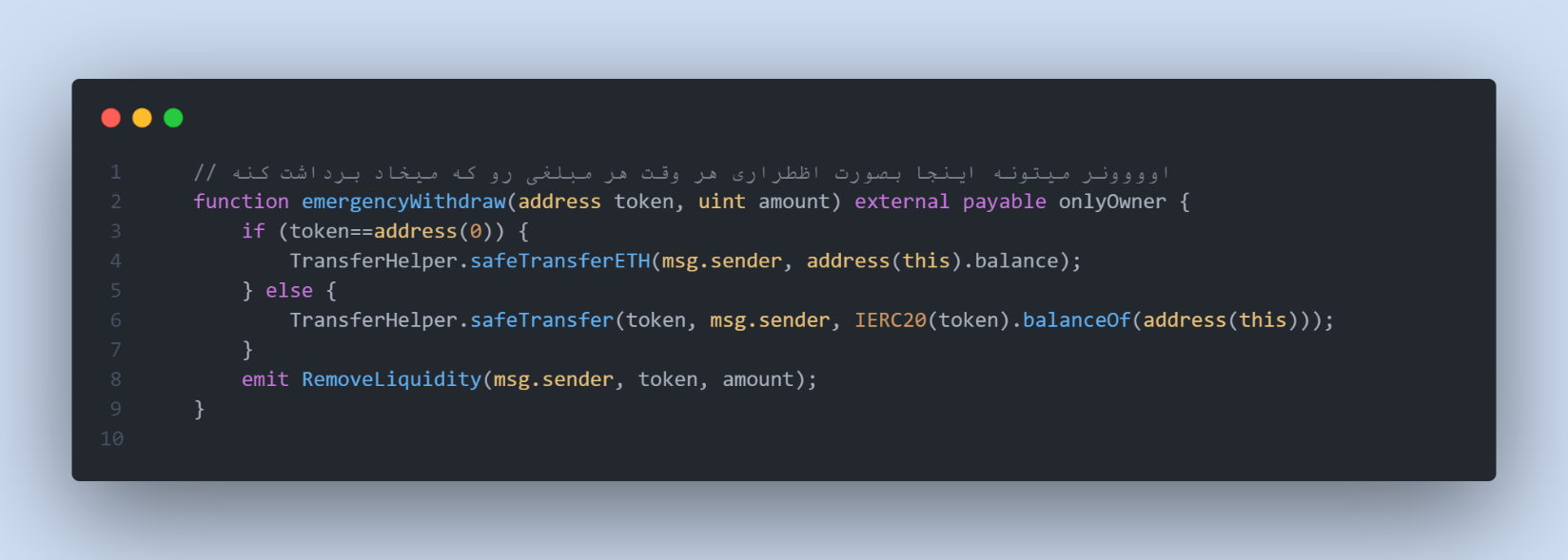
Remediation

**We recommend using the Checks-Effects-Interactions Pattern to avoid the risk of calling unknowncontracts or applying OpenZeppelin ReentrancyGuard library - nonReentrant modifier for theaforementioned functions to prevent reentrancy attack.**

* **Centralization Risks**

**In the contract Bridge the role \_owner has authority over the function emergencyWithdraw and addToken.**





Remediation

We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallet.

# **Low severity issues**

* **Missing Emit Events**

**There should always be events emitted in the sensitive functions that are controlled by centralization roles.**

Remediation

**It is recommended emitting events for the sensitive functions that are controlled by centralization roles.**