Farming Plugin Reentrancy Vulnerability

Public Incident Disclosure (Blog Post)

TL;DR: On June 12, 2025, a reentrancy vulnerability was identified in Cove's liquidity mining program and promptly neutralized. **No user funds were lost**, and **652,565 non-transferable COVE tokens** were secured as a precaution.

The vulnerability was introduced in 1inch/token-plugins@1.0.0, and was integrated by Cove. Thankfully, 1inch infrastructure was not affected: it relies on a separate version of the code.

Incident Timeline (UTC, reverse-chronological):

- **2025-06-12 13:35 UTC** – Internal review confirmed no other contracts or projects were affected; incident contained and resolved.
- **2025-06-12 04:06 UTC** – Executed a white-hat "rescue" transaction to drain and secure the remaining reward tokens, fully mitigating the vulnerability.
- **2025-06-12 01:06 UTC** – Halting of the farming rewards program via an emergency stopFarming transaction (by Cove's ops multisig) to prevent any exploitation of distributed rewards.
- **2025-06-12 00:18 UTC** – Security researcher **adriro (@adrianromero)** from **yAudit (Electi Security)** reported a flaw in the farming plugin via Immunefi; incident response was immediately initiated.

Impact Analysis

This vulnerability could have allowed an attacker to drain all reward tokens from Cove's liquidity mining program. Exactly **652,565 COVE tokens** allocated for rewards were at risk. Importantly, **no user deposits or non-reward funds were ever at risk**. Due to COVE tokens currently being non-transferable, an attacker's ability to monetize these tokens would have been severely limited. Prompt response ensured **all vulnerable reward funds were secured** before exploitation.

Root Cause

The vulnerability stemmed from a reentrancy flaw in a third-party farming plugin library (developed by 1inch) utilized for rewards distribution. A recent code optimization removed safeguards, inadvertently reintroducing a previously mitigated vulnerability. The farming plugin's balance update function could be repeatedly invoked before completion, fraudulently inflating rewards.

Actions Taken & Current Status

Upon discovery, our team immediately paused the rewards contract and executed a controlled white-hat exploit to secure the at-risk tokens. Notifications were promptly made to 1inch maintainers, and thorough reviews conducted by security partners Zellic, Pashov Audit Group (Pashov Krum), pcaversaccio, and the SEAL 911 team. The feature will stay disabled, and we will provide further updates to resuming the liquidity mining program safely in the coming weeks.

User Next Steps

No action required by users. All deposits and balances remain safe. The rewards program remains temporarily paused, and rewards will be calculated offchain in the interim so distributions are not affected. Users will be notified upon reactivation and secure redistribution of the rescued and other rewards tokens.

Acknowledgements

Special thanks to researcher **adriro (@adrianromero)** from **yAudit (Electi Security)** for responsible disclosure via Immunefi (awarded $15,000 USDC bounty). We deeply appreciate the rapid assistance from Zellic, Pashov Audit Group (Krum Pashov), pcaversaccio, Security Alliance's SEAL 911, Taylor Monahan, samczsun, 0xc0ffeebabe, Anton Bukov and the 1inch team, Robert Chen (@NotDeGhost) from OtterSec, Jazzy from Zellic (@ret2jazzy), and Josselin Feist (@Montyly), who will conduct an end-to-end security audit for Cove in July, as well as numerous others who assisted during the incident response.

Additional thanks to Storm Labs team members for triage and mitigation efforts:

- Mike Daly, Smart Contract Engineer
- John Lim, Smart Contract Lead
- Sunil Srivatsa, Founder/CEO

Forward Commitments

Security remains paramount. Cove will enhance monitoring and audit practices, accelerate migration to a more robust rewards distribution system, and refine emergency response protocols. We encourage responsible disclosures through our Immunefi bug bounty program.

Detailed GitHub Disclosure (Yearn-style)

Filename: 2025-06-12-farming-plugin-reentrancy.md

Summary

On **2025-06-12**, Cove identified and mitigated a reentrancy vulnerability in its farming rewards plugin contract derived from 1inch's ERC20 Token Plugins. A timely white-hat operation secured **652,565 non-transferable COVE tokens**. No user funds were lost, and the vulnerability has been completely neutralized.

Impact

- **Funds at Risk:** 652,565 non-transferable COVE tokens intended as rewards.
- **Losses:** None (fully secured through prompt action).
- **Affected Contract:** CoveUSD–COVE Farming Plugin.

Vulnerability Details

The flaw involved reentrancy in the _updateBalances function, lacking essential safeguards after recent code optimizations by 1inch. Malicious plugins could exploit recursive callbacks, fraudulently inflating reward balances. The protective gas-limit check was removed inadvertently, reintroducing a known risk.

Mitigation & Fix

- **Immediate Response:** Emergency halt via stopFarming; subsequent white-hat rescue secured vulnerable tokens.
- **Permanent Fix:** The team is determining the safest way to resume the rewards program and will be airdropping the reclaimed COVE and rewards tokens to users. Further communication will follow in the coming weeks.

Timeline (UTC)

- **2025-06-12 00:18** – Vulnerability reported via Immunefi by **adriro (@adrianromero)** from yAudit (Electi Security), previously audited Cove for Boosties.
- **2025-06-12 01:06** – Emergency stop executed (tx link).
- **2025-06-12 04:06** – White-hat rescue executed (tx link).
- **2025-06-12 13:35** – Incident resolved; comprehensive reviews confirmed no other vulnerabilities.

References

- Vulnerable Contract

Acknowledgements

- **Researcher:** @adrianromero (yAudit/Electi Security, via Immunefi, $15,000 USDC bounty)
- **Auditors and Security Partners:** Zellic, Pashov Audit Group (Krum Pashov), pcaversaccio, Security Alliance's SEAL 911, Taylor Monahan, samczsun, 0xc0ffeebabe, Anton Bukov, 1inch team, Robert Chen (OtterSec), Jazzy (Zellic), Josselin Feist, and numerous others
- **Storm Labs team:** Mike Daly, John Lim, Sunil Srivatsa

Contract Addresses / Commits

None

```
Vulnerable FarmingPlugin:
[0xa74e0B738b053D9083451bBAB84c538ff2Cc701d](https://etherscan.io/address/0xa74e0B738b053D9083451bBAB84c538ff2Cc701d)
```

Thread

1/ On June 12, 2025, a critical reentrancy vulnerability was identified by @adrianromero @yAuditDAO @electisec in Cove's liquidity mining program and promptly neutralized. **No user funds were lost**, and **652,565 non-transferable COVE tokens** were secured as a precaution.

The vulnerability was introduced in @1inch token-plugins@1.0.0, and was integrated by Cove. This variant was never deployed within @1inch infrastructure.

2/ An emergency halt was executed within the hour to prevent exploitation of any distributed rewards. The remaining reward tokens were then rescued via a white hat hack by the Cove team (@cyneriss @Weeb_Mcgee @devops199fan). The entire operation was completed in 3h 37m. No coveUSD funds were ever at risk.

3/ Rapid investigations were conducted by @zellic_io, @PashovAuditGrp, and @seal_911 and no further issues were found. Rescued $COVE will be airdropped to the proper users.

We're incredibly thankful to @Montyly, who is currently conducting an end-to-end security audit for Cove that includes our offchain @ApeFramework automation and fortifying our invariant test coverage.

4/ Special thanks to @adrianromero for responsible disclosure via Immunefi. We appreciate the rapid assistance from @pashovkrum @ret2jazzy @pcaversaccio @tayvano @samczsun 0xc0ffeebabe @k06a @NotDeGhost and countless others not named.

5/ Find something suspicious?

File a report via our Immunefi: https://immunefi.com/bounty/cove