Post Mortem: UIIC

Project name: UINCUBATOR
Project type: Deflationary Token
Date of exploit: 5th/6th March, 2026
Asset loss: ~$239 K
Vulnerability: wallet compromise
Date of audit conducted: 02/05/2024
Conclusion: Out of audit scope

Details of the Exploit

Project Background

UIC is a deflationary token similar to Safemoon, with a fixed supply of 21 million units and a reflection feature. Every purchase and routine transfer has a 3% fee that is automatically redistributed to holders. Sales burn 3% to a dead address, supporting the deflationary aspect. The owner can manage whitelists and control who pays fees, but ownership has now been renounced.

Nature of the Vulnerability

Attackers compromised users' wallets off-chain and, with direct control of the private keys, called transfer(to, amount) from victim addresses to move all tokens into the attacker-controlled aggregation accounts.

Timeline

March 5, 2026 – 9:45 PM EST
The UIIC team reported that multiple community user wallets had been compromised. CertiK subsequently held a call with the UIIC team to better understand the incident and discuss the initial findings.

March 5, 2026 – 10:53 PM EST
CertiK analyzed the attack path and determined that the incident was caused by a private key compromise. The attacker was able to obtain the victims' private keys and subsequently transfer the assets to addresses under their control.

March 6, 2026 – 11:37 AM EST
The UIIC team shared their internal investigation report. CertiK attended a meeting with both the team and the affected users to further analyze the potential root cause.

March 6, 2026 – 1:00 PM EST
The UIIC team initiated an investigation to determine whether a malicious version of the UIChat APK had been distributed through the project website and installed by users. The team also began reviewing the transaction signing process within the application code to ensure there are no vulnerabilities.

CertiK Audit Overview

	Detail
Skynet Profile	• https://skynet.certik.com/projects/uiic
Audit timeline	• 02/04/2024: UINCUBATOR Audit started. • 02/04/2024: Delivered the preliminary audit result, then the back-and-forth discussion on findings with the team. • 02/07/2024: CertiK Released the final report to the UINCUBATOR Team.

Audit Result	• Audit conducted in 03/06
	  ○ 13 findings
	  ○ Severity: 4 Major related to Centralization Related Risks and Inconsistency
	  ○ Status: 0 Resolved, 13 Acknowledge

Audit scope	• UIC.sol (UIC token)
Reasons for being out of scope	• The incident resulted from a private key compromise rather than a vulnerability in the smart contract. • After obtaining the private key, the attacker gained full control of the affected wallet and was able to transfer the assets to addresses under their control.

Conclusion

Based on transaction analysis and a re-evaluation of the UIC token smart contract, no vulnerabilities were identified within the audited contract that could have caused this exploit.

Evidence suggests that the incident was likely caused by private key compromise through an off-chain component.

CertiK's audit covered only the UIC token smart contract, and no issues were identified within the audited scope that could explain the incident.