



# RETROSPECT ON CNGN BASE CONTRACT DEPLOYMENT: FINDINGS AND REMEDIATION.

# TABLE OF CONTENTS

<b><u>Token Deployment Strategy.</u></b>	<b>2</b>
i. <u>Deployed contract</u>	<b>3</b>
ii. <u>Ownership transfer to our hot wallet</u>	
<b><u>Developer's Error</u></b>	<b>4</b>
i. <u>Committed Private Key</u>	
ii. <u>Commit</u>	
iii. <u>Deleted Private Key</u>	<b>5</b>
<b><u>Contract Breach</u></b>	
i. <u>Breached ownership transfer</u>	<b>6</b>
<b><u>Remediation</u></b>	
i. <u>Stakeholders Communication</u>	
ii. <u>Certik Re-Audit</u>	<b>7</b>
iii. <u>New contract address</u>	
iv. <u>Transfer of ownership to multi-sig</u>	<b>8</b>
v. <u>GitHub security</u>	
<b><u>Audit Conclusion and Summary.</u></b>	<b>9</b>



# TOKEN DEPLOYMENT STRATEGY

The token system for cNGN is made up of an Operation (access control), Forwarder, and cNGN contracts using Openzeppelin upgradeable standard and plugin, the team used a dedicated wallet (0x1BD59A8f107234A26f84746Fab7F41271C7B550e) for the deployment of contracts on the base network as well as other blockchains we currently support and then automatically, via the same deployment custom script, transferred ownership of the deployed contract to the contract admin hot wallet (0x18645845E704088da4C1bC95968E16673C540C13).

Openzeppelin upgradeable plugin tracks proxy deployments locally in the openzeppelin folder and if a ProxyAdmin is not specifically initialized with a custom owner, it deploys a default proxy admin contract with the deployer as the owner.



# DEPLOYED CONTRACT.

Block: 23861245 Confirmed by Sequencer

Timestamp: 92 days ago (Dec-18-2024 08:50:37 AM +UTC)

Transaction Action: Call 0x60806040 Method by 0x1BD59A8f...71C7B550e

Sponsored:

From: 0x1BD59A8f107234A26f84746Fab7F41271C7B550e

To: [ 0x079bf085c7fca523d04445cc0f276d93fb587223 Created ]

Value: 0 ETH (\$0.00)

Transaction Fee: 0.000005655270196427 ETH (\$0.01)

Gas Price: 0.006398912 Gwei (0.000000000006398912 ETH)

## OWNERSHIP TRANSFER TO OUR HOT WALLET

Transaction Receipt Event Logs

Address: 0x079bf085c7fca523d04445cc0f276d93fb587223

Name: OwnershipTransferred (index\_topic\_1 address previousOwner, index\_topic\_2 address newOwner) View Source

Topics: 0 0x8be0079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0

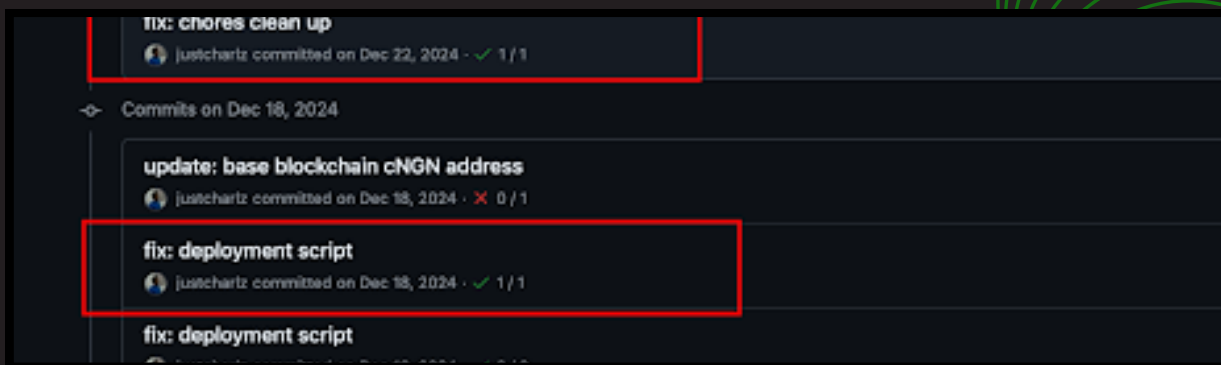
1: previousOwner Dec 0x1BD59A8f107234A26f84746Fab7F41271C7B550e

2: newOwner Dec 0x18645845E704088da4C1bC95968E16673C540C13



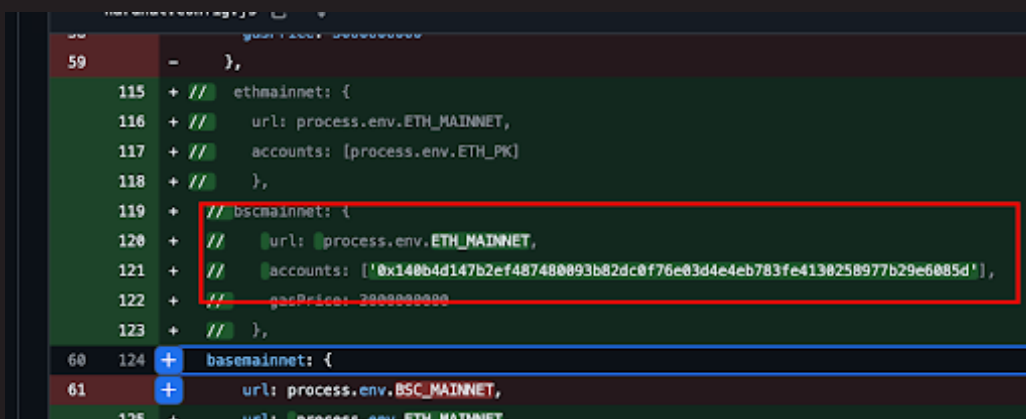
# DEVELOPER'S ERROR

On the 18th of December 2024, an erroneous commit to the organization's GitHub repo included the Private Key of the deployer address during test deployments for Base main-net. It was eventually removed as shown below but wasn't cleared from the GitHub history. This was done before Github security automation was activated.



<https://github.com/wrappedcbdc/stablecoin-cngn/commits/main/>

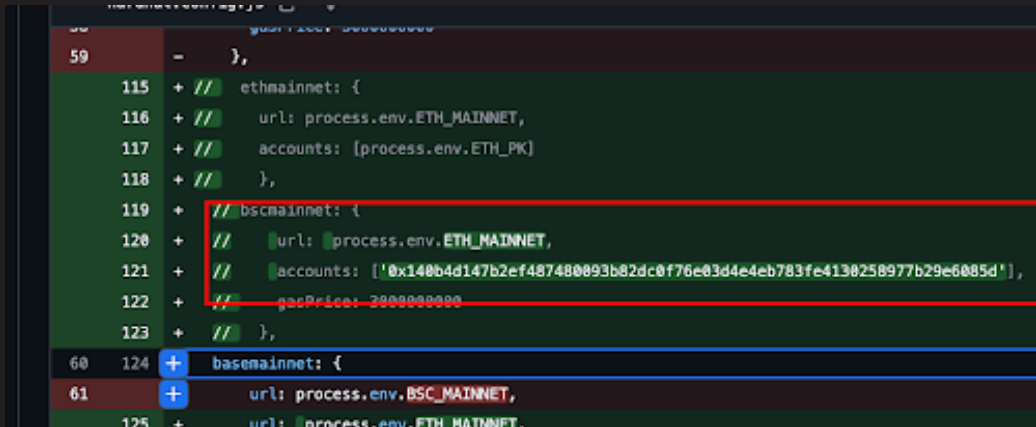
# COMMIT



<https://github.com/wrappedcbdc/stablecoin-cngn/commit/ba303d90fb99b48fa554cbe9d2bc0366153a99c1>



# DELETED PRIVATE KEY



```
59 - },
115 + // ethmainnet: {
116 + //   url: process.env.ETH_MAINNET,
117 + //   accounts: [process.env.ETH_PK]
118 + // },
119 + // bscmainnet: {
120 + //   url: process.env.ETH_MAINNET,
121 + //   accounts: ['0x140b4d147b2ef487480093b82dc0f76e03d4e4eb783fe4130258977b29e6085d'],
122 + //   gasPrice: 2000000000
123 + // },
60 124 + basemainnet: {
61 +   url: process.env.BSC_MAINNET,
125 +   url: process.env.ETH_MAINNET.
```

<https://github.com/wrappedcbdc/stablecoin-cngn/commit/ffe863b7287366d1cfbfee37a4a59c64fee6d9ac>

# CONTRACT BREACH

Due to the above error, the deployer wallet address was compromised and the transfer of ownership of the Proxy Admin Contract Owner was set to this hacker's

address(<https://basescan.org/address/0xcCfe064D2f51e83b99c666c33091ABDbE81344d8>). Research shows that the above address has been involved in other wallet breaches, as seen here.

- <https://thenewautonomy.medium.com/a-5-step-attack-process-that-crypto-projects-such-defend-against-22e427375ca6>
- <https://medium.com/@Symmetric.Finance/symmetric-incident-report-5d362f7a1a2c>
- <https://x.com/ryandemat/status/1888847663539621908>





# BREACHED OWNERSHIP TRANSFER



[https://basescan.org/tx/0x31642571d4ac275d7146ac37d05bf9e5896e57bffa907a1d493d9442a2e62b4#eventlog\\_](https://basescan.org/tx/0x31642571d4ac275d7146ac37d05bf9e5896e57bffa907a1d493d9442a2e62b4#eventlog_)

## REMEDICATION

The team had to redeploy the affected proxy cNGN contract to have control over the proxy admin contract ownership. Thereafter, transfer ownership was done to a multi-sig wallet address. This was done in line with standard procedure to ensure the security of the contract upgrades.

## STAKEHOLDERS COMMUNICATION

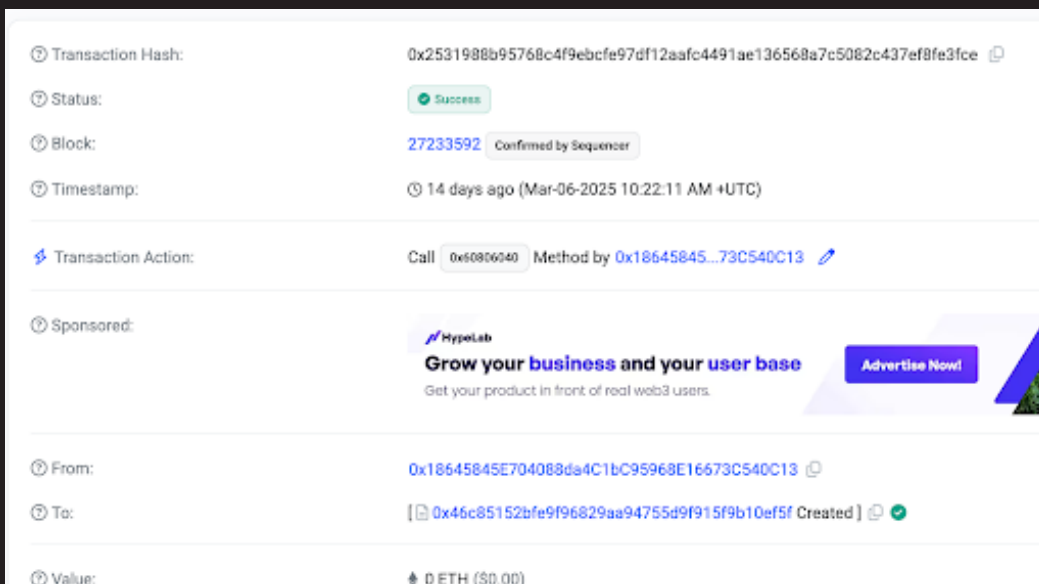
The team has communicated with all cNGN holders at the time, paused the old contract, and airdropped to the current holders who are but a few since we are still in a pilot phase.



# CERTIK RE-AUDIT

The newly deployed contract has been re-audited and awaits the final report .

## NEW CONTRACT ADDRESS



Transaction Hash: 0x2531988b95768c4f9ebcfe97df12aafc4491ae136568a7c5082c437ef8fe3fce

Status: Success

Block: 27233592 Confirmed by Sequencer

Timestamp: 14 days ago (Mar-06-2025 10:22:11 AM +UTC)

Transaction Action: Call 0x60806040 Method by 0x18645845...73C540C13

Sponsored: HypoLab  
**Grow your business and your user base**  
Get your product in front of real web3 users. [Advertise Now!](#)

From: 0x18645845E704088da4C1bC95968E16673C540C13

To: [ 0x46c85152bfe9f96829aa94755d9f915f9b10ef5f Created ]

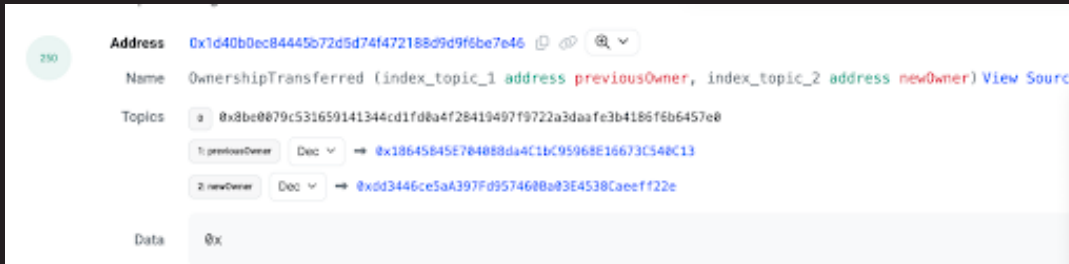
Value: 0 ETH (\$0.00)

<https://basescan.org/tx/0x2531988b95768c4f9ebcfe97df12aafc4491ae136568a7c5082c437ef8fe3fce>





# TRANSFER OF OWNERSHIP TO MULTI-SIG



<https://basescan.org/tx/0xd519b13e0cc59588234cd06650d132a6947e618bb80eda2228a2beb19c35b350#eventlog>

## GITHUB SECURITY

Code security check automation was activated for checking developers' verified commits on the cNGN repositories alongside other policies for adequate security.



# AUDIT CONCLUSION AND SUMMARY

The cNGN token system comprises multiple smart contracts using OpenZeppelin's upgradeable standard. The deployment process included automatic ownership transfers to a designated hot wallet. However, a critical security lapse occurred on December 18, 2024, when a private key was mistakenly committed to the organization's GitHub repository.

Although later removed, the exposure allowed a malicious actor to compromise the deployer wallet and gain control over the Proxy Admin contract. Upon detecting the breach, the team took swift remediation steps by redeploying the affected contract and transferring ownership to a multi-signature wallet for improved security.

The incident was effectively communicated to stakeholders, and cNGN token was airdropped to holders according to their snapshot holdings. A security re-audit by Certik has been initiated for the new contract.

To prevent future incidents, the use of Foundry cast for deployment as a way of protecting private keys and prevent a reoccurrence. GitHub security automation was activated to monitor commits and enforce stricter security policies. Additionally, we are planning for bug-bounty, and other corrective measures to enhance contract security and mitigate similar risks.

## Signed and Approved

David Uzochukwu  
*Lead Auditor, Guild Audits*

Charles Okaformbah  
*Technical Lead, cNGN*

