// HALBORN

RandLabs - MyAlgo Wallet

Executive Summary

Prepared by: **Halborn**

Date of Engagement: **March 7th, 2023 - April 7th, 2023**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	04/11/2023	Guillermo Muñoz
0.2	Document Updates	04/13/2023	Guillermo Muñoz
0.3	Document Review	04/13/2023	Gabi Urrutia
1.0	Final Document	04/14/2023	Guillermo Muñoz
1.1	Final Document Review	04/14/2023	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

RandLabs engaged Halborn to conduct an incident triage on their infrastructure and underlying assets beginning on March 7th, 2023 and ending on April 7th, 2023. The Halborn team was given a period of one month to carry out the engagement and had three security engineers devoted full-time to analyze the incident that occurred.

These security engineers are experts in smart-contract security and blockchain, possessing advanced skills in penetration testing, smart-contract hacking, and a comprehensive understanding of several blockchain protocols.

1.2 OBJECTIVES AND SCOPE

This engagement was executed with the intent of discovering any potential data leakage that could potentially compromise the security of users' private keys, identifying potential security issues within the RandLabs infrastructure and identifying potential vulnerabilities on MyAlgo code-base. As part of the scope, the following assets were evaluated:

- Github: Multiple repositories associated with MyAlgo repository were reviewed manually and automatically. Additionally, all the GitHub actions deployed between October 2022 and February 2023 were reviewed manually.
- CDN: The CDN Management Account's Audit Logs were provided for a period of 18 months in order to clarify the correlation in between the potentially compromised API key and the user's account activity.
- Cloud Security Provider: Based on the investigation, the Cloud Security Provider was briefly inspected to identify possible signs of compromise (IoCs).
- Telemetry: The RandLabs team granted access to the Telemetry application, enabling the analyst to conduct a thorough investigation into potential information leaks associated with the service.
- JS File: Halborn team analyzed the content of the malicious Javascript file.
- Google Analytics: The Halborn team looked into suspicious evidence and potential indicators of compromise (IoCs).
- Web Vulnerabilities: Multiple scenarios were examined; however, only a Client-side vulnerability was assessed as having the requisite capabilities for accessing the data storage.

1.3 EXECUTIVE SUMMARY

The CDN API key linked to a particular account was potentially compromised, jeopardizing the account's security. Exploiting the potentially compromised API key, a malicious actor introduced harmful JavaScript code into a web application via a specific worker of the CDN.

The perpetrator extracted users' confidential data, including private keys and mnemonics, by transmitting POST requests to a particular domain containing the acquired sensitive information. Consequently, the attacker managed to obtain users' mnemonics and private keys by engaging with the compromised website, potentially enabling unauthorized access to users' digital assets.

Therefore, the following final considerations of the incident triage are deducted:

- The attack was performed using a potentially compromised CDN API key.
- It was highly unlikely to determine how the CDN API key was obtained with the information available to Halborn at the time of the engagement.
- The Github codebase didn't contain any security vulnerabilities or bugs that could have been misused.
- There was no evidence that the users' account was compromised.

For the time being, law enforcement is still investigating the incident for further clarification.

THANK YOU FOR CHOOSING

// HALBORN