CredShields
Audit Report

Sept 6th, 2023 • CONFIDENTIAL

Description

This document details the process and result of the security audit performed by CredShields Technologies PTE. LTD. on behalf of Primestack Pte. Ltd between **July 14th, 2023**, and **July 31st, 2023**.

Author

Shashank (Co-founder, CredShields)

shashank@CredShields.com

Reviewers

Aditya Dixit (Research Team Lead)

aditya@CredShields.com

Prepared for

Primestack Pte. Ltd

1. Executive Summary

Primestack engaged CredShields to perform a Black box mobile application pentest of Okto (iOS and Android) from July 14th, 2023, to July 31st, 2023. During this timeframe, nine (9) vulnerabilities were identified.

During the audit, zero (0) vulnerabilities were found that had a severity rating of either High or Critical. These vulnerabilities represent the greatest immediate risk to "Primestack" and should be prioritized for remediation.

The table below shows the in-scope assets and a breakdown of findings by severity per asset. *Section 2.3* contains more information on how severity is calculated.

	Critical	High	Medium	Low	Info	Σ
Okto Mobile Applications	0	0	1	6	2	9
	0	**0**	**1**	**6**	**2**	**9**

Table: Findings Overview

The security audit was conducted by the CredShields team to focus on identifying vulnerabilities in Okto Mobile Applications (Android & iOS) scope during the testing window while abiding by the policies set forth by Primestack.

Maintaining a healthy security posture requires constant review and refinement of existing security processes. Running a CredShields audit allows Primestack's internal security team and development team to uncover specific vulnerabilities and better understand the current security threat landscape.

Reviewing the remaining resolved reports for a root cause analysis can further educate Primestack's internal development and security teams and allow manual or automated procedures to be put in place to eliminate entire classes of vulnerabilities in the future. This proactive approach helps contribute to future-proofing the security posture of Primestack's assets.

2. Methodology

Primestack engaged CredShields to perform a black box security audit of Okto Mobile Applications (iOS and Android). The following sections cover how the engagement was put together and executed.

2.1 Preparation phase

In contrast to the preparatory phase described in grey box pentesting, black box pentesting approaches the assessment of a mobile application without any prior access to internal documents or system information. In black box pentesting, CredShields' team operates with a limited knowledge of the application's inner workings, relying solely on the publicly available information and the mobile app itself. This approach simulates the perspective of an external attacker with no internal insights. The team initiates the testing process by interacting with the application as an end user, exploring its features, and probing for vulnerabilities without any prior knowledge or mapping of the logic flow. This methodology aims to assess the application's security posture in a manner that closely mimics real-world attack scenarios, allowing for a comprehensive evaluation of its resilience to external threats.

A testing window from July 14th, 2023, to July 31st, 2023, was agreed upon during the preparation phase.

2.1.1 Scope

During the preparation phase, the following scope for the engagement was agreed upon:

ASSETS IN SCOPE
Asset 1: **Android Application** **https://play.google.com/store/apps/details?id=com.coindcx.okto** **Asset 2:** **iOS Application** **https://apps.apple.com/us/app/okto-wallet/id6450688229**

Table: Asset(s) in Scope

2.1.2 Audit Goals

Audit procedures at CredShields involve both automated (in-house) tools and manual analysis. However, the majority of audit methods require a manual review of the application's source code.

The testing was done in accordance with the standards of the OWASP MASTG, along with an extended self-developed checklist based on industry standards. The team focused heavily on the core concept behind all the functionalities, along with preparing test and edge cases. This included understanding the business logic and how it could have been exploited.

2.2 Retesting phase

Primestack is actively partnering with CredShields to validate the remediations implemented towards the discovered vulnerabilities.

2.3 Vulnerability Classification and Severity

Discovering vulnerabilities is important, but estimating the associated risk to the business is just as important.

To adhere to industry guidelines, CredShields follows OWASP's Risk Rating Methodology. This is calculated using two factors - **Likelihood** and **Impact**. Each of these parameters can take three values - **Low**, **Medium**, and **High.**

These depend upon multiple factors such as Threat agents, Vulnerability factors (Ease of discovery and exploitation, etc.), and Technical and Business Impacts. The likelihood and the impact estimate are put together to calculate the overall severity of the risk.

CredShields also defines an **Informational** severity level for vulnerabilities that do not align with any of the severity categories and usually have the lowest risk involved.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Overall, the categories can be defined as described below -

1. **Informational**

   Informational vulnerabilities aren't urgent concerns. Instead, they offer opportunities to enhance code quality, emphasizing readability and best practices. They don't pose direct threats but suggest valuable improvements that don't fit into other severity categories. Code maintainers should decide whether to address these issues based on their judgment.

2. **Low**

   Vulnerabilities in this category pose minimal risks to both the product and the organization. These risks are relatively small and may not be exploited frequently. Alternatively, the client may consider them insignificant, considering their specific business situation.

3. **Medium**

   Medium-severity issues often result from weak or flawed code logic. They have the potential to compromise the privacy of end-users by exfiltrating or altering their private information. In specific, unforeseen situations or conditions beyond the adversary's control, such vulnerabilities could harm the client's reputation. It is essential to address these issues within a defined timeframe and remediation cycle.

4. **High**

   High-severity vulnerabilities pose a significant threat to mobile app security. They can result in a partial compromise of user data or system functionality, potentially

causing harm to both the app and the organization. Exploiting these vulnerabilities might require some level of sophistication, and they can damage the app's reputation. Immediate attention and remediation are necessary.

5. Critical

Critical mobile app security issues are directly exploitable vulnerabilities that can compromise users' sensitive information without needing any external conditions to be met. These vulnerabilities pose a significant risk to a large number of users and can lead to severe damage to the client's reputation and financial consequences.

6. Appendix 1

6.1 Disclosure:

The Reports neither endorse nor condemn any specific project or team nor do they guarantee the security of any specific project. The contents of this report do not, and should not be interpreted as having any bearing on, the economics of tokens, token sales, or any other goods, services, or assets.

Emerging technologies such as Blockchain, Smart Contracts, or anything in Web3 carry a high level of technical risk and uncertainty. There is no warranty or representation made by this report to any Third Party in regards to the quality of code, the business model or the proprietors of any such business model, or the legal compliance of any business.
In no way should a third party use these reports to make any decisions about buying or selling a token, product, service, or any other asset. It should be noted that this report is not investment advice, is not intended to be relied on as investment advice, and has no endorsement of this project or team. It does not serve as a guarantee of the project's absolute security.
CredShields Audit team owes no duty to any third party by virtue of publishing these Reports.