NETTITUDE
AN LRQA COMPANY

Penetration Testing Findings Summary

Prepared For: AZETS
Target: MOBILE APPLICATIONS
Author: AARON THACKER
Date: 11 May 2022

Confidential Security Document

1 Findings

1. Mobile Application

Component	Description	Severity	Recommendation	Status
Please refer to the finding.	No Obfuscation	Medium	It is recommended that the source code is obfuscated when building production releases.	Not Remediated
Please refer to the finding.	Open Redirection	Medium	Ensure that unapproved client provided URLs are not incorporated into any redirect function.	Remediated
Azets Cozone (Android) Azets Cozone Employee (Android)	Android Signature Bypass via Janus Attack	Low	Update the minimum SDK version to API level 24 or above and disable the v1 signature scheme if compatibility with older devices is not needed.	Not Remediated
Azets Cozone (iOS) Azets Cozone Employee (iOS)	Jailbreak Detection Bypassed	Low	Implement a multi-level jailbreak detection strategy.	Partially Remediated
Azets Cozone (Android) Azets Cozone Employee (Android)	Root Detection Bypassed	Low	Implement a multi-level root detection strategy, including common cloaking applications and rooting artefacts.	Not Remediated
Azets Cozone (iOS) Azets Cozone Employee (iOS)	No TLS Certificate Pinning	Low	Implement a TLS certificate pinning strategy taking into consideration Nettitude's recommendations.	Not Remediated

Please refer to the finding.	No Tamper Detection	Low	Implement tamper detection mechanisms.	Not Remediated
Azets Cozone (iOS) Azets Cozone Employee (iOS)	Insecure State Transition	Low	Disable the application snapshot from being displayed in the recent apps list.	Remediated
https://idp-develop-proddb.staging.cozone.com/api/v1/oauth2/revoke	Insufficient Session Expiration	Low	Ensure the ‘logout' function within the application destroys the authentication token client-side and server-side.	Remediated
Azets Cozone (Android) Azets Cozone Employee (Android)	Android External Storage Permitted	Informational	Consider using Android's internal storage to store sensitive data.	Partially Remediated