DIRECTDEFENSE

Teton Simulation

API Security Assessment Summary Report

Prepared By:
DirectDefense, Inc.
Date:
October 2, 2020

TABLE OF CONTENTS

ENGAGEMENT SUMMARY

Teton Simulation enlisted the services of DirectDefense to perform a comprehensive API security assessment of the organization's SmartSlice API.

The goal of the engagement was to review Teton Simulation’s API for external threats that could affect the API's overall security posture in a negative way and provide guidance and strategic support to resolve any identified issues.

OVERALL THREAT EXPOSURE

FINDINGS SUMMARY

Overall Teton Simulation has shown a good level of understanding when it comes to implementing security within their external (Internet-facing) API. This engagement revealed that, while some weaknesses do exist within the API, they posed a low to moderate risk. The issues identified during this assessment may pose a threat to application confidentiality; however, exploitation opportunities are minimal. Remediating the findings discussed within the technical report will further strengthen the tested systems and applications.

Identified Strengths:

- **Proper Input Validation** -- DirectDefense observed proper server-side validation of all inputs into the API. This helps prevent injection attacks against the server-side components and protect the backend databases and support systems.
- **Strong Authorization Controls** -- Throughout the course of the application assessment, authorization controls were checked to ensure the API did not disclose other users' data or deliver data to unauthorized users. Similarly, API functionality did not allow users to amend settings for which they did not have authorization.
- **Sufficient Token Randomness** -- During the assessment, DirectDefense identified that token values used to identify sessions and grant authorization to the API were sufficiently randomized to avoid prediction-based attacks from potential malicious actors.
- **Rate Limiting** -- The application incorporates rate limiting on all end points. This mitigating control slows down attackers, granting monitoring systems more time to notice malicious behavior and take action.
- **Quick Developer Action** -- During the assessment, several of the findings disclosed by DirectDefense through daily updates were addressed by the development team the following day. Developers quickly addressed any identified weaknesses.

Teton Simulation administrators and security team are already in the process and planning stages for closing the issues that were identified. Findings are to be remediated in order of evaluated risk posed in conjunction with the probability of attack.

SCOPE AND METHODOLOGY

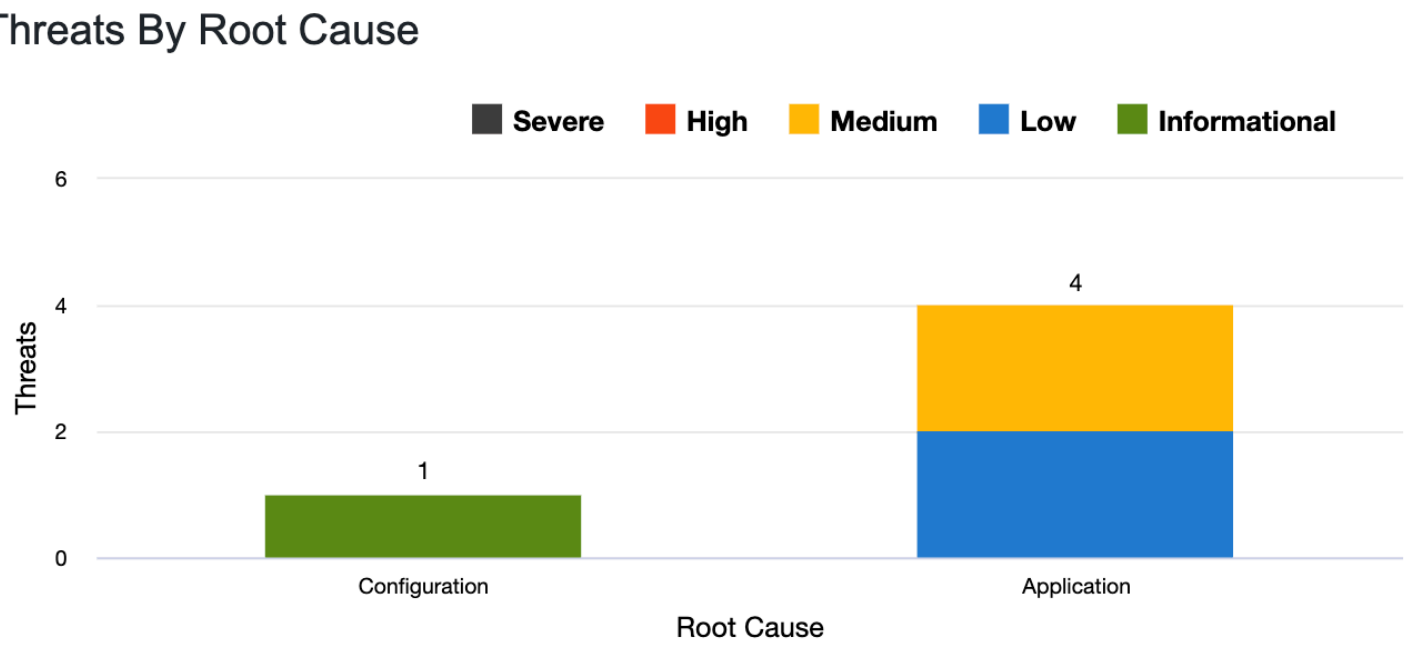
DirectDefense consultants follow a phased assessment approach that is extremely effective for testing and improving the security of applications and APIs. This method identifies an organization's tactical and strategic security challenges by taking a technical snapshot of the current security posture and then analyzing the technical controls and processes that will affect that posture for the long term.

The following table outlines the phases and associated components of the engagement that were executed for Teton Simulation:

EXTERNAL EXPOSURE - SECURITY TESTING PHASES
Application Programming Interface (API) Assessment This phase of the security assessment focused on the security of applications in scope for the assessment. During this phase, DirectDefense consultants used a comprehensive set of tools, custom scripts, and manual techniques to thoroughly identify possible threats to the application. Like a traditional application penetration test, all identified threats were tested and validated to evaluate the depth of compromise and risk of exposure. Unlike a traditional penetration test, this evaluation of threats was not isolated or limited to a handful of threats, but rather across all threats identified within the application tested.

CURRENT THREAT DISTRIBUTION

To aid in the understanding of where threats lie within the organization and the root cause issues that were discovered, the following charts display the distribution of threats among the primary threat vectors tested, threats based on DirectDefense's controls mappings to show where root cause issues lie within the environments, and finally a breakout of threats based on phases of the assessment.



CONCLUSIONS

Customers and business partners of Teton Simulation can be assured that proper due diligence has been carried out by a third-party security firm. Testing was done independently to evaluate Teton Simulation's external networking environments and supporting applications from an information security standpoint. Based on the findings observed, and the remediation plan submitted to Teton Simulation, the external networking environments and supporting applications are only a few steps away from following a security best practices approach.