Security Audit Summary

Tuple Platform (Web Backend & macOS Application)

Prepared for **Tuple, Inc.**
Prepared by: **John Villamil**
06/09/2020

Executive Summary

Overview

Tuple, Inc. engaged Doyensec to perform a security assessment of the Tuple platform. The project commenced on 05/06/2020 and ended on 05/15/2020 requiring one (1) security researcher.

The project consisted of a manual application security assessment for the both macOS application and the web backend.

Testing was conducted remotely from Doyensec EMEA and US offices.

Scope

Through meetings with Tuple, Inc., the scope of the project was clearly defined. We list the agreed upon assets below:

- Tuple macOS application
- Ruby On Rails backend

The testing took place in both staging and production environment using the latest version of the software at the time when testing started.

In detail, this activity was performed on the following releases:

- https://github.com/tupleapp/backend
  - 2b7e026e63dd634c8b9d135b30925d36739d4ce9
- https://github.com/tupleapp/macapp
  - a83f247e41191f68327a96c9fee04c24a392fbf3

Scoping Restrictions

During the engagement, Doyensec did not encounter any difficulties in testing the application. The macOS application staging build was not working properly and so, when it was necessary, the production build and environment instead were used instead.

While the SSO feature was not in the initial scope, this credential type was assigned a day before the engagement concluded. We did not perform a comprehensive evaluation of this component.

Findings Summary

Doyensec researchers discovered and reported ten (10) vulnerabilities in the Tuple platform. While several issues are departure from best practices and low-severity flaws, Doyensec identified one (1) issues rated as High that can be leveraged to compromise the platform.

It is important to reiterate that this report represents a snapshot of the security posture of the product at a point in time.

All issues have been addressed in a timely manner by Tuple, Inc. None of the outstanding security vulnerabilities discovered during this engagement exist.

Overall, the security posture of the Tuple platform was found to be in line with industry best practices.

Methodology

Overview

Doyensec treats each engagement as a fluid entity. We use a standard base of tools and techniques from which we built our own unique methodology. Our 30 years of information security experience has taught us that mixing offensive and defensive philosophies is the key for standing against threats, thus we recommend a graybox approach combining dynamic fault injection with an in-depth study of source code to maximize the ROI on bug hunting.

During this assessment, we have employed standard testing methodologies (e.g. OWASP Testing guide recommendations) as well as custom checklists to ensure full coverage of both code and vulnerabilities classes.

Setup Phase

Tuple Inc. provided access to the application in scope, the online environment and the source code repository.

Tooling

When performing assessments, we combine manual security testing with state-of-the-art tools in order to improve efficiency and efficacy of our effort.

During this engagement, we used the following tools:

- Burp Suite
- LLBD
- Dtrace
- Frida

Web Application and API Techniques

Web assessments are centered around the data sent between clients and servers. In this realm, the principle audit tool is the Burp Suite, however we also use a large set of custom scripts and extensions to perform specific audit tasks. We focus on authorization, authentication, integrity and trust. We study how data is interpreted, parsed, stored, and relayed between producers and consumers.

We subvert the client with malicious data through reflected and DOM based Cross Site Scripting and by breaking assumptions in trust. We test the server endpoints for injection style flaws including, but not limited to, SQL, template, XML, and command injection flaws. We look at each request and response pair for potential Cross Site Request Forgery and race conditions. We study the application for subtle logic issues, whether they are authorization bypasses or insecure object references. Session storage and retrieval is scrutinized and user separation is thoroughly tested.

Web security is not limited to popular bug titles. Doyensec researchers understand the goals and needs of the application to find ways of breaking the assumed control flow

About Doyensec

Doyensec was founded in 2017 by John and Luca who are its only stakeholders. The company exists to further the passion and focus of its creators. We aim to provide research-driven application security, enabling trust in our client's products and evolving the resilience of the digital ecosystem.

With offices in the US (San Francisco) and Europe (Warsaw), Doyensec has access to a unique talent pool of security experts capable of providing worldwide consulting services.

US Office

350 Townsend Street, Suite 840
94107 San Francisco
California, United States

John Villamil
john@doyensec.com
+1 609 349 2941

EMEA Office

Ul. Florianska 6, Suite 1B
03-707 Warsaw
Poland

Luca Carettoni
luca@doyensec.com
+48 883 555 069

For any inquiries, please contact info@doyensec.com

We keep a small dedicated client base and expect to develop long term working relationships with the projects and people involved. We will find bugs, but we know that is just the first step in the process. At any stage of your security maturity, you can rely on Doyensec to solve your unique application security needs.

We value and rely on the following principles:

- **Passion**. We believe quality comes from passion and care. We love what we do, and continuously work on mastering our craft. Every engagement is finely executed with dedication and attention to details.
- **Expertise**. Our team has decades of experience in application security. We are industry leaders in penetration testing, reverse engineering, and source code review. Doyensec researchers have discovered numerous vulnerabilities in widely-deployed products, secured fortune 500 enterprises, advised startups and worked with tech companies to eradicate security flaws.
- **Focus**. Security craftsmanship is all about individual attention and delivering tailored security services and products. We concentrate on application security and do fewer things, better.
- **Research**. The fast changing landscape of technologies and security threats requires constant innovation. We are dedicated to providing research-driven application security and therefore invest 25% of our time in building security testing tools, discovering new attack techniques and developing countermeasures.