INTRODUCTION

From April 3 to May 15, 2017, Confide's applications were audited, inspected and analyzed for a security assessment by Positive Technologies. This assessment was conducted by multiple security engineers and analysts from Positive Technologies. The purpose of the assessment was to identify potential application security issues and to demonstrate how these issues could be exploited. The scope of the evaluation included Confide's server, mobile and desktop applications. Upon completion of the security assessment, Positive Technologies provided detailed recommendations to Confide alongside each of the findings.

This statement is to confirm and to detail that Confide's applications have been thoroughly reviewed and evaluated by Positive Technologies. This document reflects Positive Technologies' assessment of Confide's overall security posture during the timeframe referenced above. Security techniques and threats are constantly changing and, as such, this document does not make any representation about the current security measures against future threats.

METHODOLOGY

The evaluation was performed using a combination of black-box, gray-box, and white-box methodologies. Security engineers and analysts from Positive Technologies used a wide variety of proprietary and publicly available tools, as well as manual techniques throughout the assessment. During the evaluation, Confide provided their source code as well as access to engineers to answer questions.

During the course of the assessment, Confide's code was inspected following the standards and best practices recommended by organizations such as the Web Application Security Consortium (WASC) and the Open Web Application Security Project (OWASP).

The following methods were used:

- **Black-box testing** performed on behalf of an external attacker with no direct access to the application. The black-box technique is web application security testing carried out without any "inside" knowledge of the application.
- **Gray-box testing** performed on behalf of an authorized user with standard privileges. This technique provides for additional data that the Service Provider receives from the Customer, such as credentials and access points to log in as an ordinary Customer's client.
- **White-box testing** performed on behalf of an attacker with access to the application source code.

SUMMARY OF FINDINGS

During the assessment, Positive Technologies found no critical or high severity issues and a small number of medium and low severity issues. All findings were reported to Confide along with recommendations. After the security assessment concluded, a validation assessment of the remediation was performed. As of May 19th, 2017, all issues reported to Confide have been properly addressed.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

info@ptsecurity.com ptsecurity.com