KNOWLEDGE consulting group KCG

THE GOVERNMENT'S TRUSTED ADVISOR

Agiloft

Application Remediation Test
Executive Summary Report
10/22/2013

WWW.KNOWLEDGECG.COM
PLAZA AMERICA TOWER II · 11710 PLAZA AMERICA DR. · SUITE 520 · RESTON, VA 20190 · (703) 467-2000

Legal Notice

© Knowledge Consulting Group
All rights reserved 2013
This document contains confidential and proprietary information. It is intended for the exclusive use of Agiloft. Unauthorized use or reproduction of this document is prohibited. KCG assures that findings in this report are true to the extent that can be verified via the Internet. This Executive Summary Report reveals all relevant vulnerabilities known up to the date of this report. As new vulnerabilities continue to be found and the introduction of new security threats, it is suggested that security assessments be conducted after every major change in the Information System and periodically in 3 to 6 month intervals.

Security Consultants

Name	Company	Function	Email
Shawn Evans	KCG	Sr. Penetration Tester	Shawn.Evans@Knowledgecg.com
Charles Riggs	KCG	Sr. Penetration Tester	Charles.Riggs@Knowledgecg.com
Chris Littlebury	KCG	Sr. Penetration Tester	Chris.Littlebury@Knowledgecg.com

Reviewers

Name	Company	Function	Email
Andrew Whitaker	KCG	Director, Cyber Attack Penetration Division	Andrew.Whitaker@Knowledgecg.com

Contact

For more information about this document and its contents please contact Knowledge Consulting Group.

Name	Andrew Whitaker
Address	11710 Plaza America Dr. Suite 520 Reston VA 20190
Phone	(503) 489-7289
E-mail	Andrew.Whitaker@Knowledgecg.com

Summary

Agiloft, Inc. (Agiloft) engaged KCG Cyber Attack and Penetration Division (CAPD) to perform a penetration assessment from the perspective of an external hacker. The engagement was in two phases. During the first phase that concluded on 10/04/2013, KCG designed the engagement to provide an independent assessment of the web application's security posture and provided Agiloft with findings/recommendations. Agiloft acted on these in preparation for the second phase of testing by KCG that concluded on 10/23/2013 with an updated set of findings/recommendations. This summary details the findings and recommendations of the second phase of testing.

This remediation assessment evaluated the effectiveness of Agiloft's efforts to remediate findings discovered in an application penetration test that was completed on 10/04/2013. During the penetration test, KCG performed a wide variety of automated and manual tests using a selection of tools, techniques, and methodologies. There were five (5) findings discovered during the original assessment. During the second phase of the assessment, KCG evaluated the overall effectiveness of Agiloft's remediation efforts to address these risks.

The overall risk rating for Agiloft is low.

Agiloft has demonstrated due diligence in remediating the previously discovered findings. All of the previous findings were thoroughly tested and found to be non-existent. Agiloft has followed industry best practices to quickly and effectively address all findings. Additionally, no new risk was discovered during the timeframe of the remediation assessment.

Assessment Objectives

Scope

For both phases, targets of evaluation were limited to the following:

Internet Protocol (IP) Addresses	Hostnames	Uniform Resource Locator (URL)
72.172.176.130	ew-130.agiloft.com	https://ew-130.agiloft.com/gui2/

Phase 1: Penetration Test

At the request of Agiloft, KCG performed a security assessment of Agiloft's web application. The purpose of this assessment was to identify security issues as well as vulnerabilities affecting specific services and devices of the organization. The objective of the analysis was to simulate an attempted attack and assess Agiloft's security posture.

KCG's assessment methodology includes structured review processes based on recognized "best-in-class" practices as defined by such methodologies as the Institute for Security and Open Methodologies (ISECOM's), Open Source Security Testing Methodology Manual (OSSTMM), the Open Web Application Security Project (OWASP), and ISO 27001 Information Security Standard.

Overall, the consultants discovered five (5) findings. KCG provided Agiloft with tactical and strategic recommendations to address the immediate issues and to have long-term controls in place to prevent these findings in future code revisions.

Phase 2: Remediation Assessment

After Agiloft addressed the findings, KCG performed a remediation assessment of Agiloft's web application. The purpose of this assessment was to evaluate the effectiveness of Agiloft's remediation efforts to address findings discovered in a previous penetration test assessment. Additionally, KCG tested to verify that new risks were not introduced with the remediation efforts.

KCG consultants determined that all findings were adequately addressed. KCG was unable to reproduce any of the previous findings and did not discover any new findings during the remediation assessment.

End of Report.