Application Vulnerability Assessment for the LivePerson Real-time Engagement Platform

Introduction

AppSec Labs has successfully carried out a vulnerability assessment and application penetration testing of the LivePerson real-time engagement application and web platform.

The tests were designed to evaluate the security and immunity of the following components:

- *LivePerson Web Admin Console*
- *LivePerson Agent Console*
- *LivePerson Monitor tag (mTag)*

AppSec Labs performed the security testing against the applications and platform to attempt and determine the extent to which a potential attacker can view, alter, or delete information without proper authorization. AppSec Labs utilized several test accounts created by LivePerson for the testing. AppSec Labs attempted to view and modify information between these test accounts without utilizing the passwords and appropriate authentication controls for the accounts. AppSec Labs also attempted to circumvent the assigned user access rights and gain access to functionality not otherwise authorized for access. AppSec Labs tested the platform by using both standard user privileges and administrator user privileges.

Methodology

AppSec Labs developed a customized process for conducting Ethical Hacking assessments of applications. AppSec Labs has created a documented, proprietary methodology for conducting these tests. Tests that AppSec Labs has performed as part of the Web Application Ethical Hacking assessment include, but are not limited to, the following:

- *Strength of the session credentials used by type: URL rewriting, cookies, hidden form elements and HTTP authentication (Basic, NTLM, Digest, etc.). AppSec Labs tested for the predictability of session tokens to check, whether it is subject to manipulation, cloning, or hijacking and other common weaknesses in the mechanism employed to track user sessions.*

- *Improper configuration of the Web server, possibly resulting in directory indexing, default scripts and executables (with known vulnerabilities), and the ability to use HTTP methods/verbs such as PUT and DELETE without authorization.*

- *Strength and proper logic flow of server executables (.CGI, .ASP, .ASPX, .PHP, Cold Fusion, PERL, etc.), and the lack of proper bounds checking, which can lead to buffer overflow attacks, as well as Denial of Service (DoS) attacks.*

- *Review of HTML source for common vulnerabilities, such as excessive information in comments, and the use of GET commands versus POST commands. Hidden form elements were also reviewed for information disclosure or as sources of input into the application server.*

- *Strength of the login functions against common attacks such as username enumeration/harvesting and password brute-forcing. Proper and complete use of the logout and timeout functions will also be tested.*

- *Examination of SSL encryption use. Proper use of strong algorithms, minimum key length and other relevant data relating to the encryption process.*

- *Analysis of all information passed across the communication channel between the client software and the server. AppSec Labs has captured information, and attempted to manipulate and replay the information that has been captured. In addition, AppSec Labs has attempted to modify the client-server network communication in real-time where possible.*

- *Appropriate use of warnings and error messages and browser warnings such as unsigned code, AutoComplete, etc.*

- *Review of vulnerabilities for cross account access violations (accessing other customer's data), DOS/DDSOS and all known versions of XSS.*

- *Tests to identify vulnerabilities based on OWASP Top 10*

- *Various commercial, publicly available, and AppSec Labs developed proprietary tools were used for testing.*

Upon completion of the testing, AppSec Labs presented all identified vulnerabilities/risks to LivePerson in a detailed final report. Each vulnerability or risk identified was categorized as critical, high, medium, or low, as follows:

Critical Risk	*These findings expose major security risk with a direct exploit. If exploited, the security threat might cause major damage to the network, system or application. The likelihood of such attack to occur is high, considering the architecture/business logic/complexity of the exploit.*
High Risk	*These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or information, but the likelihood to occur is not high, considering the architecture/business logic/complexity of the exploit. The possible damage to the application or the company is high, but not crucial.*
Medium Risk	*These findings identify conditions that do not immediately or directly result in the compromise or unauthorized access of a network, system, application, or information, but do provide a capability or information that could, in combination with other capabilities or information, result in the compromise or unauthorized access of a network, system, application, or information.*
Low Risk	*These findings identify conditions that do not immediately or directly result in the compromise of a network, system, application, or information, but do provide information that could be used in combination with other information to gain insight into how to compromise or gain unauthorized access to a network, system, application, or information. Low risk findings may also demonstrate an incomplete approach to or application of security measures within the environment.*

Consolidated Findings Summary

AppSec Labs has submitted an Application Security testing assessment report with all the findings to LivePerson.

Based on the results of re-testing and verification process completed on July 2014, AppSec Labs confirms that there are ***no open Critical-Risk, no open High-Risk and no open Medium-Risk*** *vulnerability identified at this time.*

Cautionary Note

The vulnerability assessment that AppSec Labs performed was based on past experiences, currently available information, and known threats as of the date of testing. Given the constantly evolving nature of information security threats and vulnerabilities, there can be no assurance that any assessment will identify all possible vulnerabilities, or propose exhaustive and operationally viable recommendations to mitigate those exposures.

The statements relevant to the security of the Admin Console applications, Agent Console and Monitoring Tag in this letter reflect the conditions found at the completion of testing.

In accepting our report on the Web application and application, LivePerson has acknowledged the validity of the above cautionary statement. AppSec Labs also strongly recommends that any network, information system, or online application be subject to periodic reassessment and policy review, in addition to complementary training of the key support personnel on such policies and procedures for the above infrastructure in order to maintain a strong security profile in the face of potential threats.

Shai Gans, VP Security Services,

AppSec Labs

July 2014