Attestation of Application Security Assessment

Jama Software, Inc.

November 21, 2016
Disclaimer

This document contains and constitutes the proprietary and confidential information of GuidePoint Security, LLC, (“GuidePoint”). It is provided to Jama Software, Inc. (“Jama”) subject to and in accordance with the terms of any agreement between GuidePoint and Jama regarding treatment of confidential information and/or licensing of proprietary information. This document also contains information that is the highly sensitive confidential information of Jama and should be treated by representatives of Jama accordingly. The recipient, without the express permission of GuidePoint and Jama, may not distribute this document.

The contents of this document do not constitute legal advice. GuidePoint’s offers of services or deliverables that relate to compliance, litigation, or other legal interests are not intended as legal counsel and should not be taken as such.
Independent Security Assessment Report

To Whom It May Concern:

GuidePoint Security, LLC ("GuidePoint") has performed an Application Security Assessment for Jama Software, Inc. ("Client") while acting as an independent security assessor. This assessment was performed with the intent of evaluating the scope, security, and resiliency of Client’s Jama application environments. GuidePoint found no Critical or High severity level findings during the final assessment.


While this type of assessment is intended to mimic a real-world attack scenario, GuidePoint is bound by rules-of-engagement, defined scope, allocated time, and additional related constraints. GuidePoint has made every effort to perform a thorough and comprehensive analysis and to provide appropriate remedial advice. However, inherent limitations, errors, misrepresentations, and changes to the Client environment may have prevented GuidePoint from identifying every security issue that was present in the Client environment at the time of testing. Therefore, the findings included in this report should be considered to be representative of what a similarly skilled attacker could achieve with comparable resources, constraints, and time frame.

Additionally, it is worth emphasizing that the findings and remediation recommendations are the result of a point-in-time assessment based on the state of the Client environment as of April 27, 2016. GuidePoint therefore does not provide any assurance related to configuration or control modifications in the Client environment, changes in regulatory or compliance requirements, discoveries of new vulnerabilities and attack techniques, or any other future event that may impact the Client’s security posture.

The information contained in this report represents a fair and unbiased assessment of the Client’s environment based on the agreed upon criteria as defined in the Statement of Work. This report is provided to the Client as notification of outstanding security risks that threaten the confidentiality, integrity, and availability of sensitive information, as well as to provide assistance and direction with remediation. The evidence and references provided for each finding serve as the basis for our qualified opinions in this report.

GuidePoint has provided this report solely for private and internal use by the Client, and it may not be shared or redistributed without GuidePoint’s express written consent. GuidePoint’s assessments focus exclusively on information security and the conclusions arrived at in this report should not be considered to be a representation or endorsement of the Client’s products or services.

Bryan Orme
Principal
GuidePoint Security

GuidePoint Security, LLC.
2201 Cooperative Way
Suite 225
Hemdon, VA 20171
(877) 889-0132
info@guidepointsecurity.com
www.guidepointsecurity.com

Copyright © 2016 GuidePoint Security, LLC, All Rights Reserved
Executive Summary

Background

Jama Software, Inc. ("Jama") engaged GuidePoint Security ("GuidePoint") to perform an Application Security Assessment of Jama’s web application. An Application Security Assessment is comprised of Application Penetration Testing, and supporting Infrastructure Penetration Testing. These assessment activities utilize automated and manual security testing techniques to identify vulnerabilities and weaknesses within the target application, its supporting infrastructure, and client components.

An Application Penetration Test analyzes the dynamic (runtime) functionality of an application and attempts to identify security deficiencies by abusing and misusing that functionality. Whenever possible, GuidePoint performs testing from the perspective of multiple application roles since attacks may originate from anonymous, unauthenticated users, malicious authorized users, or attackers that have compromised authorized accounts.

The following list summarizes the activities performed as part of the Jama Application Security Assessment.

- Dynamic Analysis
  - Automated Application Vulnerability Analysis
  - Unauthenticated (Anonymous) Application Penetration Testing
  - Authenticated (Credentialed) Application Penetration Testing

Note: Denial-of-Service (DoS) testing was not in-scope for this engagement.