Date: March 16, 2021
From: Black Hills Information Security
Subject: Security Assessment for Rapid7 Web Application Insight VM

Background

From January 11, 2021 to February 19,2021 Rapid7 contracted Black Hills Information Security to perform a security assessment of their web application "Insight VM". The objective of this assessment was to identify security risks and suggest remediation strategies to reduce risk to critical business data related to the web application.

The testing process began with an overview of the use cases of the target systems in which Black Hills information security consultants learned the legitimate uses and identified potential threat vectors and hypothetical exploitation models. Automated and manual testing techniques were used to assess the target areas to gauge the level of business risk of any discovered vulnerabilities. This letter is a point in time analysis of the target environment.

Web Application Testing

- Form fields and request parameters checked for input validation
- Identify SQL Injection
- Identify Cross-Site Scripting (XSS) and Cross-Site Request Forgery
- Identify known command injection vulnerabilities
- Identify known vulnerabilities in common commercial and open-source web application software
- Identify Business Logic errors in applications
- Attempt to exploit vulnerabilities found in an effort to gain access to the target host

Assessment Methodology

Our assessment was a point in time review of the security controls of a particular web application or application components. There were five major phases conducted within the assessment: discovery, automated testing, manual testing, findings analysis, and documentation. These five phases allowed Black Hills Information Security consultants to conduct a security examination of the target network range while gathering the required information to properly rank and prioritize the threats for the client. Specifically, the assessment evaluated the extent to which externally accessible systems were designed to:

- Ensure the security and confidentiality of information;
- Protect against anticipated threats or hazards;
- Protect against unauthorized access to or use of information.

Our Assessment was performed by CISSP and GIAC certified Consultants using a methodology based on industry best practices such as ISO 17799, NSA-IAM, OWASP and OSSTMM.

General Findings and Opinion

In our opinion, the accompanying discussion presents fairly, in all material respects, the areas we evaluated and their corresponding security status. Also, in our opinion, Rapid7 appears to maintain sufficient security controls, vulnerability levels and general security practices that comply with industry best practices to create a secure web application. While we cannot guarantee that a security breach will never occur, it is our overall opinion that Rapid7 has taken the appropriate steps to reduce their enterprise risk level and mitigate the probability of such an event.

Concluding Remarks

Based on the assessment, Rapid7 has implemented sufficient security controls to the continued operation of business processes. The existing security controls adequately mitigate risks to business processes to ensure the protection of personally identifiable information and customer data. To this end, Rapid7 appears to meet the common best practices for a secure web application.

Use of This Document

This document has been prepared solely for the use of Rapid7 (the "Company", Rapid7), and its officers, directors and employees (collectively with the Company, "Company Entities"). No other third party shall be entitled to rely upon this document. The provision of this document or information herein to the parties other than Company Entities, shall not entitle such parties to rely on this report or the contents thereof in any manner or for any purpose whatsoever, and Black Hills Information Security Inc. specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) arising from or related to provision of such report or information to such parties.

Sally Vandeven

Sally Vandeven
Senior Security Analyst
Black Hills Information Security