Date: April 7, 2025
From: Black Hills Information Security
Subject: Security Assessment for NetFoundry

Background

From March 10 to March 18, 2025, NetFoundry contracted Black Hills Information Security (BHIS) to perform a security assessment of their Ziti API. The objective of this assessment was to identify security risks and suggest remediation strategies to reduce risk to critical business data for NetFoundry's external-facing IT assets.

The testing process began with an API mapping phase in which BHIS consultants gathered knowledge of the application, its components, and its critical functions.

BHIS then created potential threat vectors and developed and tested hypothetical exploitation models. Automated and manual testing techniques were used to assess the target areas to gauge the level of business risk posed by any discovered vulnerabilities. This letter is a point-in-time analysis of the target API.

Web Application Testing Conducted

- Tested effectiveness of input validation
- Probed for
    - SQL Injection
    - Command injection vulnerabilities
    - Vulnerabilities in third-party web application software
    - Authorization and Business logic errors in functionalities
- Attempted to exploit each identified vulnerability

Assessment Methodology

This BHIS assessment was a point-in-time review of the security controls of the client API. The assessment comprised five major phases: discovery and mapping the attack surface, automated testing, manual testing, findings analysis, and documentation. These five phases allowed BHIS consultants to conduct a security examination of the target networks while gathering the required information to properly rank and prioritize the threats for the Ziti API. Specifically, the testers evaluated the extent to which the API had been built to do the following:

- Safeguard the security and confidentiality of information
- Protect against anticipated threats or hazards
- Defend against unauthorized access to or use of information

BHIS assessments are performed by CISSP and GIAC certified consultants or under the supervision of certified consultants. BHIS testers use a methodology based on the industry's best practices such as NIST Special Publication 800-115, Penetration Testing Execution Standard, NSA-INFOSEC Assessment Methodology, Open Web Application Security Project, and the Open-Source Security Testing Methodology Manual.

General Findings and Opinion

In our opinion, the accompanying discussion presents fairly, in all material respects, the evaluated areas and their corresponding security status. Also, from our perspective, the API appears to maintain sufficient security controls, vulnerability levels and general security practices that align with industry best practices to reduce environmental risk. While BHIS cannot guarantee that a security breach will never occur, we estimate that

NetFoundry has taken reasonable steps to address enterprise risk level and reduce the probability of a significant incident.

Use of This Document

This document has been prepared solely for the use of NetFoundry (the “Company”, NetFoundry), 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.

Fernando Panizza
Lead Penetration Tester
Black Hills Information Security