NCC Group
650 California St, Suite 2950
San Francisco, CA 94108
https://nccgroup.com

March 2, 2022

RSA Security
174 Middlesex Turnpike
Bedford, MA 01730

Introduction

Between the days of January 24th and February 25th, 2022, three (3) consultants from NCC Group expended sixty(60) person-days of effort on a black box transactional web assessment against the RSA NetWitness application.

The purpose of this assessment was to identify application-level security issues that could adversely affect the integrity of RSA NetWitness application. This assessment was performed by NCC Group under the guidelines provided in the statement of work for the engagement.

Testing Methods

The scope of the assessment included the following components:

- Infrastructure/Platform
- NetWitness UI
- Security
- Investigation
- NetWitness Core
- Respond
- Administration
- UEBA
- Endpoint
- Integration Service
- Reporting
- Correlation Service
- Log Collector
- NW Live content management
- ContextHub
- Malware
- Health and Wellness
- License Server

While evaluating the security of the RSA NetWitness application, NCC Group attempted to perform the following:

- Determine a security stance based on identified vulnerabilities
- Compromise integrity of sensitive data
- Attempt injection vectors such as command injection, XSS, CSRF, SSRF and other OWASP-type issues which may impact the individual components or downstream functionality
- Execute privileged commands remotely
- Obtain confidential information
- Attempt to compromise key components from the vantage point of a malicious actor within either the network or an individual component
- Scan for vulnerabilities using open source and commercial tools
- Manually inspect identified hosts, ports, and services
- Fuzzing core service binaries and web endpoints
- Review overly permissive firewall rules
- Identify misconfigured, vulnerable, out-of-date, and end-of-life servers and application platforms
- Demonstrate vulnerability to public exploits, including exploiting non-disruptive vulnerabilities
- Determine a security stance based on identified vulnerabilities and deployment configurations

Upon completion of the assessment, all findings were reported to RSA.