RSA Security, LLC
174 Middlesex Turnpike
Bedford, MA 01730

Introduction

Between the days of July 17th and July 26th, 2023, two (2) consultants from NCC Group engaged in a Web Application and Web Service Security test for a total of thirteen (13) person-days of effort reviewing RSA Security, LLC's NetWitness application.

The purpose of this assessment was to identify application-level security issues that could adversely affect the security of the 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:

- Log Collector, Packet Collector, Endpoint Collector
- Log Decoder, Network Decoder, Endpoint Decoder
- Concentrator, Archiver

- Microservices: Investigate, Respond, Source, Content, Orchestrator, Admin, Security, Licensing, Local Repo Update, Config, Reporting Engine, Integration

- NetWitness UI (or Platform XDR)
- Event Stream Analysis (Correlation)
- UEBA Cloud and On-premises
- NetWitness Insight
- Risk Scoring

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

- Identify issues related to communication security, error handling, and data exposure
- Identify and exploit vulnerabilities such as Cross-Site Scripting and SQL Injection
- Compromise integrity of sensitive data or obtain unauthorized access
- Examine for weaknesses in session management authentication
- Examination for Server Side Include injection attacks
- Examination for file upload vulnerabilities as well as downloading unauthorized files
- Examination for arbitrary code execution or compromising other machines
- Escalate privileges or bypass key business logic rules
- Examination against any previously known issues
- Evaluate the overall security stance based on identified vulnerabilities

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