July 20th, 2023

To whom it may concern,

In March – May 2023, Assured Information Security, Inc. (AIS) conducted a functional, operational, and security assessment of the Neoflow product. Testing and evaluation (T&E) consisted of validating the technology's overall functionality, identifying potential vulnerabilities in credential workflows and their associated communications, and evaluating the privacy implications associated with the use of the technology.

T&E was conducted remotely against the Neoflow web portal as well as the application programming interface (API), by a team of security specialists, guided by the industry accepted standard NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Based on this standard, T&E was a structured process, following four phases:

- **Planning** – This involves defining the scope (a subnet, application, datacenter, etc.), rules (White Box, Black Box, etc.), schedule and other parameters and goals.
- **Discovery** – This involves gathering information that will be used for the attack. Potential targets, vulnerabilities and exploits are identified. Discovered assets are compared against known vulnerability databases to assist penetration testing efforts.
- **Attack** – This involves the attempted exploitation of targets, based on discovered information.
- **Reporting** – This involves the documentation of successful exploits, and their corresponding vulnerabilities and assets. Reporting occurs throughout the penetration testing process.

During this test, systems and assets were targeted using the methods most likely to be used by today's cybercriminals. The T&E team met with Neoflow personnel to establish and document the testing scope, and subsequently were given a fixed period of time to attempt the compromise of targeted assets. The attack portion of the engagement attempted exploitation of vulnerabilities identified during the discovery phase, using industry recognized tools. Testing tools utilized include:

- **NMAP** - network mapping, custom packet configuration, vulnerability discovery
- **cURL -** a tool to transfer data from or to a server, using one of the supported protocols
- **Burp Suite** - a proxy-based tool used to evaluate the security of web-based applications and do hands-on testing
- **Wireshark -** an open-source network protocol analyzer
- **Nikto -** an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items
- **Custom generated scripts**

Based on the results of the test, AIS provided Neoflow a detailed report containing testing process, identified controls, and recommendations to further improve their security posture. After remediation by the Neoflow team, AIS testing confirmed that no identified security weaknesses remained outstanding at the close of the assessment (i.e., zero critical, high, medium or low severity items).

AIS provides government and commercial customers with industry-leading cyber and information security capabilities specializing in research, development, consulting, testing, forensics, remediation, and training. Headquartered in Rome, New York, the company strives to be a driving force for technology and national security through our innovative solutions, unprecedented capabilities, and groundbreaking research.

Should you have any questions on the matter at hand or would like to personally discuss, please reach out to myself or the AIS team.

Regards,

Brandon Haines
hainesb@ainfosec.com
Neoflow Test Team Lead
Systems Analysis and Exploitation | Assured Information Security, Inc.