NewLine.ai

January 2022

Product Security

Domain:
newline.ai

301 Government Center Drive
Suite 200
Wilmington, NC 28403

T (910) 208-4612
F (910) 660-0935

1 | Product Security

NewLine values the work done by security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify, reproduce, and respond to legitimate reported vulnerabilities. If any vulnerabilities are to be found, please contact us at cs@newline.ai.

2 | Responsible Disclosure Guidelines

We will investigate legitimate reports and make every effort to quickly correct any vulnerability. To encourage responsible reporting, we will not take legal action against you nor ask law enforcement to investigate you provided you comply with the following Responsible Disclosure Guidelines:

- Provide details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC). Any vulnerability that implicates functionality not resident on a research-registered vehicle must be reported within 168 hours and zero minutes (7 days) of identifying the vulnerability.
- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our services.
- Do not modify or access data that does not belong to you.
- Give NewLine a reasonable time to correct the issue before making any information public.
- Alter only areas that you have permission to access.
- Do not compromise the safety of the software or expose others to an unsafe condition

3 | Physical Security

The NewLine's production infrastructure is hosted in Cloud Service Provider (CSP) environments. Physical and environmental security related controls for NewLine production servers, which includes buildings, locks or keys used on doors, are managed by these CSP's.

4 | Corporate Security

NewLine leverages internal services that require transport level security for network access and individually authenticate users by way of a central identity provider and leveraging two factor authentication wherever possible.

All NewLine personnel undergo regular security and privacy awareness training that weaves security into technical and non-technical roles; all employees are encouraged to participate in helping secure our customer data and company assets. Security training materials are developed for individual roles to ensure employees are equipped to handle the specific security oriented challenges of their roles.

5 | Authentication and Access Management

End users may log in to NewLine using an Identity Provider. This service will authenticate an individual's identity and may provide the option to share certain personally identifying information with NewLine, such as your name and email address to pre-populate our sign up form.

All requests to the NewLine API must be authenticated. Requests that write data require at least reporting access as well as an API key. Requests that read data require full user access as well as an application key. These keys act as bearer tokens allowing access to NewLine service functionality.

6 | Protection of Customer Data

Data submitted to the NewLine service by authorized users is considered confidential. This data is protected in transit across public networks and encrypted at rest. Customer Data is not authorized to exit the NewLine production service environment, except in limited circumstances such as in support of a customer request.

All data transmitted between NewLine and NewLine's users is protected using Transport Layer Security (TLS) and HTTP Strict Transport Security (HSTS). If encrypted communication is interrupted the NewLine application is inaccessible.

Access to Customer Data is limited to functions with a business requirement to do so. NewLine has implemented multiple layers of access controls for administrative roles and privileges. Access to environments that contain Customer Data requires a series of authentication and authorization controls, including Multi-Factor Authentication (MFA). NewLine enforces the principles of least privilege and need-to-know for access to Customer Data, and access to those environments is monitored and logged for security purposes. NewLine has implemented controls to ensure the integrity and confidentiality of administrative credentials and access mechanisms, and enforces full-disk encryption and unique credentials for workstations.