Response to nVisium Audit

We enlisted the independent security firm nVisium to audit the design and architecture of the new End-to-End Encryption feature of Day One. We were pleased with the professionalism and thoroughness of the audit process.

In summary, the audit identified a few non-critical vulnerabilities. Our actions and plans in response to these items are listed below.

Identified vulnerabilities

Lack of Key Rotation for Certain Cryptographic Keys (Medium Risk)

Details: The application architecture did not account for key rotation for critical keys like the user's master key and private key.

Response: Key rotation will be supported in a future release but not initially. As an interim workaround, a user who is concerned about potentially compromised keys may clear their synced data entirely from our servers and then re-encrypt and re-upload their journal data from their local device. Please contact support for instructions on how to do this.

Insufficient Cache Control (Medium Risk)

Details: The application allowed clients and intermediate proxy servers to cache an unnecessary amount of user information.

Response: We have rectified this situation, and now have the proper cache controls in place for our application.

User Password Passed as Query Parameter (Medium Risk)

Details: User credentials were exposed as query parameters during authentication attempts.

Response: We have rectified this situation for our recent client releases. User credentials are now passed in the body of a POST request.

Lack of a Forced App Update Process (Medium Risk)

Details: The architecture did not have a process to force critical application updates.

Response: We acknowledge this issue and are discussing how to address it.

Certificate Pinning Not Implemented (Low Risk)

Details: The application relied upon the local device's Certificate Authority (CA) trust chain to determine if HTTPS connections were trustworthy and secure**.**

Response: We acknowledge this issue and are discussing how to address it.

Lack of Process to Manage Software Dependencies (Low Risk)

Details: The application architecture lacked a software dependency management process.

Response: The team will work to improve our processes so that we stay on top of security updates in the third-party dependencies used in our products.

Lack of Process for Abuse Complaints (Low Risk)

Details: The application did not have a process to accept or process abuse complaints.

Response: This item may have been due to a miscommunication between Day One staff and the audit team as we have a process in place. In addition to our normal customer support channels, Day One has a dedicated email address, security@dayoneapp.com, to receive complaints and inquiries about security and privacy issues, including abuse. The client apps have built-in tools for quickly contacting customer support. Abusive user accounts can also be disabled by Day One.