Security Audit by Doyensec Q3 2020
Actions taken

This document outlines the actions taken by Basecamp to address Doyensec team's findings in the HEY apps. For a recap of the 21 issues flagged, please refer to pages 7 and 8 of the security audit report.

Summary

From the 21 issues found by Doyensec:

- 3 were classified as 🔴 **high-severity**, and we fixed the 3 of them.
- 7 were classified as 🟠 **medium-severity**, and we fixed 6 of them but decided not to address the remaining one.
- 10 were classified as 🟡 **low-severity**. We fully fixed 8 of them, partially addressed 1 of them, and decided not to address the remaining one.
- 1 was classified as ℹ️ **informational**. We didn't address it.

Read below for more details about our changes and the reasons for them.

Detailed actions taken

1. CSP Bypass in Script-Src Directive - 🟡 low-severity

We fixed this by removing the offending CDN, cdn.syndication.twimg.com, from our CSP.

2. Hard-coded Credentials In Various Components - 🟡 low-severity

We fixed this in two ways:

- We removed the hard-coded credentials from the source code except for those that weren't critical credentials.
- We invalidated the existing password that was included in the iOS app by relying on a different authentication mechanism for the protected resource, which didn't include sensitive information in any case. The password is still in the app but it doesn't correspond to any resource. It'll be removed a future version of the app.

3. Missing Certificate Pinning on iOS, Android and Electron Apps - 🟠 medium-severity

We evaluated this and decided not to implement it as it would make it difficult to change our certificates. Existing clients would stop working until there was an update and might be non-trivial to update a legacy app we might no longer be working on, as it has happened with other apps because of our "Until the Internet" stance (https://basecamp.com/about/policies/until-the-end-of-the-internet).

4. Password Reset Token Could Be Reused Multiple Times - 🟡 low-severity

We fixed this one by restricting password reset tokens to be used once, within their validity period.

5. 2FA Bypass Via Mobile Endpoints - 🟠 medium-severity

We applied the same strict rate limit to OAuth endpoints as the one we apply in the web endpoints to address this issue.

6. Content Spoofing Via Attachment Type - 🟡 low-severity

We fixed this one by only allowing valid attachment types in filter.

Basecamp

Security Audit by Doyensec Q3 2020
Actions taken

7. Stored Cross Site Scripting (XSS) On The Gopher Image Proxy - 🟡 low-severity
We fixed this one by removing support for SVG images in our image proxy.

8. Blind Server Side Request Forgery Via Gopher Image Proxy - 🟠 medium-severity
We mitigated this one on the image proxy, forbidding all accesses to internal addresses.

9. Missing Snapshot Overlay and FLAG_SECURE On Every Activity and Fragment on iOS and Android Apps - 🟡 low-severity
We decided not to address this one due to the low risk and the damage that a fix would inflict on user experience and usability. It'd prevent the multi-tasking UI from displaying the app's contents, for example.

10. Insufficient Deletion of Application Data on iOS, Android and Electron Apps - 🟡 low-severity
We addressed this in the Android app, which now removes all data when the app is uninstalled, but it's not yet addressed on the iOS and Electron apps.

11. Exposed Internal Endpoints For Various Components - 🟡 low-severity
We didn't address this one as the exposed internal endpoints discovered were harmless and used for monitoring and other tasks that required them to be publicly accessible.

12. hey.com Dependencies With Known Vulnerabilities - 🟡 low-severity
We updated all dependencies and set up a step in our CI builds to alert us of new vulnerabilities in our dependencies.

13. Haystack Dependencies With Known Vulnerabilities - 🟡 low-severity
Same as above.

14. Open Redirect Abusing Referer - ℹ️ informational
We decided not to address this one per its complexity compared to its informational nature.

15. Weak ContentProvider Implementation Leads to Attachments Stealing on Android App - 🟠 medium-severity
We fixed this one in our Android app.

16. IP Address Leak Via Cascading Style Sheet Injection - 🟠 medium-severity
We fixed this one and any other bypasses of our proxy by preventing non-proxied resources (styles, fonts, images) from being loaded via our CSP.

17. Missing contextIsolation Flag On Electron App - 🔴 high-severity
We fixed this one.

Basecamp

Security Audit by Doyensec Q3 2020
Actions taken

18. No Restrictions for HTML5 Media APIs on Electron App - 🟠 medium-severity

We fixed this one in our Electron app.

19. OpenExternal Insecure Usage on Electron App - 🔴 high-severity

We fixed this one in our Electron app.

20. Arbitrary Navigation via locationIsInternal on Electron App - 🟠 medium-severity

We fixed this one in our Electron app.

21. Rails Active Storage Delivery Method Proxy - 🔴 high-severity

We fixed this one directly in Rails: https://github.com/rails/rails/pull/40149