HEY

Security Assessment

October 22, 2021

Prepared for:
Rosa Gutiérrez
Basecamp

Prepared by:
Claudia Richoux
Jim Miller
Alex Useche

About Trail of Bits

Founded in 2012 and headquartered in New York, Trail of Bits provides technical security assessment and advisory services to some of the world's most targeted organizations. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code. With 80+ employees around the globe, we've helped secure critical software elements that support billions of end users, including Kubernetes and the Linux kernel.

We maintain an exhaustive list of publications at https://github.com/trailofbits/publications, with links to papers, presentations, public audit reports, and podcast appearances.

In recent years, Trail of Bits consultants have showcased cutting-edge research through presentations at CanSecWest, HCSS, Devcon, Empire Hacking, GrrCon, LangSec, NorthSec, the O'Reilly Security Conference, PyCon, REcon, Security BSides, and SummerCon.

We specialize in software testing and code review projects, supporting client organizations in the technology, defense, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, and Zoom.

Trail of Bits also operates a center of excellence with regard to blockchain security. Notable projects include audits of Algorand, Bitcoin SV, Chainlink, Compound, Ethereum 2.0, MakerDAO, Matic, Uniswap, Web3, and Zcash.

To keep up to date with our latest news and announcements, please follow @trailofbits on Twitter and explore our public repositories at https://github.com/trailofbits. To engage us directly, visit our "Contact" page at https://www.trailofbits.com/contact, or email us at info@trailofbits.com.

Trail of Bits, Inc.
228 Park Ave S #80688
New York, NY 10003
https://www.trailofbits.com
info@trailofbits.com

Notices and Remarks

Classification and Copyright

This report is public at the request of Basecamp. It may be viewed on Trail of Bits' public repository and wherever Basecamp chooses.

Test Coverage Disclaimer

All activities undertaken by Trail of Bits in association with this project were performed in accordance with a statement of work and mutually agreed upon project plan.

Security assessment projects are time-boxed and often reliant on information that may be provided by a client, its affiliates, or partners. As such, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Table of Contents

Executive Summary

Overview

Basecamp engaged Trail of Bits to review the security of the HEY encryption approach and a brief review of their mobile application. From June 4 to June 12, 2020, a team of Trail of Bits consultants conducted a security review of the client-provided source code, with two person-weeks of effort. Details of the project's timeline, test targets, and coverage are provided in subsequent sections of this report.

Project Scope

We focused our testing efforts on the identification of flaws that could result in a compromise or lapse of confidentiality, integrity, or availability of the target system. We performed automated testing and a manual review of the code, in addition to running system elements for dynamic analysis.

Summary of Findings

The audit uncovered three defects that could impact system confidentiality, integrity, or availability. We identified three high-severity issues:

- Encrypted data could be recovered due to repeated nonces in AES-GCM.
- Database storage could be susceptible to deserialization attacks.
- The lack of guardrails could lead to encryption library misuse.

EXPOSURE ANALYSIS

Severity	*Count*
High	3
Medium	10
Low	9
Informational	0
Undetermined	0

CATEGORY BREAKDOWN

Category	*Count*
Access Controls	1
Configuration	7
Cryptography	5
Data Exposure	7
Data Validation	2

Project Summary

Contact Information

The following managers were associated with this project:

Dan Guido, Account Manager
dan@trailofbits.com

Cara Pearson, Senior Project Manager
cara.pearson@trailofbits.com

The following engineers were associated with this project:

Claudia Richoux, Consultant
claudia.richoux@trailofbits.com

Project Timeline

The significant events and milestones of the project are listed below.

Date	Event
June 4, 2020	Project pre-kickoff call
June 8, 2020	Status update meeting
June 16, 2020	Delivery of report draft
June 16, 2020	Report readout meeting

Project Goals

The engagement was scoped to provide a security assessment of the Basecamp application. Specifically, we sought to answer the following non-exhaustive list of questions:

- Can attackers access or alter email data?
- Can database content be recovered in the event of a compromise?
- Can attackers bypass the application's authentication?
- Does the database encryption design use safe and modern cryptographic primitives?
- Is the database encryption design susceptible to any known cryptographic attacks?
- Are there any flaws or weaknesses in the application's key management?
- Are there any low-complexity issues in the Android and iOS applications that can be identified?

Project Targets

The engagement involved a review and testing of the targets listed below. We were also provided with a compiled IPA and APK for dynamic analysis of the mobile application.

Actiontext

Repository	https://github.com/basecamp/actiontext
Version	4017f1e
Type	Ruby
Platform	Web

Haystack

Repository	https://github.com/basecamp/haystack/blob/
Version	7b1a9f2-
Type	Ruby
Platform	Web

Project Coverage

This section provides an overview of the analysis coverage of the review, as determined by our high-level engagement goals. Our approaches and their results include the following:

- We manually reviewed the `active_record_encryption` database encryption gem, focusing on the following:
  - The database-level encryption scheme design
  - The use of encryption as it pertains to the goals listed in the data inventory
  - Cryptographic choices, possible weaknesses, and vulnerability to cryptographic attacks
  - The system's key management
- We manually reviewed the authentication flow in Android, iOS, and web clients, including OAuth and Transport Layer Security (TLS) configurations.
- We manually reviewed the attachment storage in S3.
- We manually reviewed the differences between the development and production configurations.
- We ran Brakeman against the codebase and triaged the results.
- We briefly reviewed the Android and iOS applications for environmental and configuration concerns.

Coverage Limitations

Due to the time-boxed nature of the audit, we focused our review on key components of the application that could result in high-impact vulnerabilities for Basecamp. In this case, our main focus was on the database encryption design and on cryptographic best practices.

Mobile Testing Results

The table below summarizes our review of the HEY mobile applications on iOS and Android.

Title	Type	Severity
Android ID Collected	Data Exposure	Medium
Google Play Warning: GCP API Keys Exposed in App	Data Exposure	Medium
Weak ECB Mode Used for Symmetric Encryption	Cryptography	Medium
Enable Verification on Android Security Provider	Configuration	Medium
Server Lacks OCSP Stapling	Configuration	Medium
Disable Third-Party Keyboards	Configuration	Medium
App Store Blocker: Dangerous ATS Exemptions	Configuration	Medium
App Susceptible to URI Scheme Hijacking	Configuration	Medium
Hash Generated Using Broken Cryptography API (SHA1)	Cryptography	Medium
Message Digest Generated Using Broken Cryptography API	Cryptography	Medium
Enable SafetyNet Attestation API	Configuration	Low

Data Dumped to 3rd Party OSS/SDK - Google Services	Data Exposure	**Low**
App Views are Vulnerable to TapJacking	Configuration	**Low**
Enable Android Verify Apps	Configuration	**Low**
File Access Enabled Within WebView	Access Controls	**Low**
Switch to Write-Only Access to User's Photo Library	Data Exposure	**Low**
Data Dumped to 3rd Party OSS/SDK - Sentry	Data Exposure	**Low**
Utilize More Private Photo Access APIs	Data Exposure	**Low**
Utilize More Private API to Access User's Contacts	Data Exposure	**Low**

Summary of Findings

The table below summarizes the findings of the manual code review, including type and severity details.

ID	Title	Type	Severity
1	Deterministic encryption is flawed	Cryptography	High
2	Database storage is vulnerable to deserialization attacks	Data Validation	High
3	Lack of guardrails to protect against the misuse of the encryption library	Cryptography	High

Summary of Recommendations

Trail of Bits recommends that Basecamp address the findings detailed in this report, focusing on the implementation of cryptographic best practices across the code base. Furthermore, given the limited time alloted for this audit, we suggest planning a comprehensive review of the application's back end, focusing on application security concerns such as authentication and authorization controls, data validation, and error handling.

A. Vulnerability Categories

The following tables describe the vulnerability categories, severity levels, and difficulty levels used in this document.

Vulnerability Categories	
Category	**Description**
Access Controls	Insufficient authorization of users or assessment of rights
Auditing and Logging	Insufficient auditing of actions or logging of problems
Authentication	Improper identification of users
Configuration	Misconfigured servers, devices, or software components
Cryptography	Breach of the confidentiality or integrity of data
Data Exposure	Exposure of sensitive information
Data Validation	Improper reliance on the structure or values of data
Denial of Service	System failure with an availability impact
Error Reporting	Insecure or insufficient reporting of error conditions
Patching	Outdated software package or library
Session Management	Improper identification of authenticated users
Testing	Insufficient test methodology or test coverage
Timing	Race conditions, locking, or other order-of-operations flaws
Undefined Behavior	Undefined behavior triggered within the system

Severity Levels	
Severity	**Description**
Informational	The issue does not pose an immediate risk but is relevant to security best practices or defense in depth.
Undetermined	The extent of the risk was not determined during this engagement.
Low	The risk is relatively small or is not a risk the client has indicated is important.
Medium	Individual users' information is at risk; exploitation could pose reputational, legal, or moderate financial risks to the client.
High	The issue could affect numerous users and have serious reputational, legal, or financial implications for the client.