Codecov

Code coverage done right.®
https://codecov.io

Infrastructure Vulnerability Assessment

Version: Codecov Enterprise v4.3.0
By: Stephen Peak - CEO

OVERVIEW

This document serves as an assessment of Codecov Enterprise's infrastructure, concerning security and vulnerability of system components.

DEFINITIONS

1. Distribution: the Codecov Enterprise compiled release.
2. Machine: the server in which your Distribution runs. It contains the volumes associated with the archives and databases.
3. Administrator: a person who has Secure Shell (SSH) access to the Machine.
4. Upload: a collection of coverage reports uploaded to Codecov.
5. Provider: the source control tool connected to Distribution (e.g., GitHub Enterprise).
6. OAuth Tokens: used to access the Provider's API. They are issued from the Provider.
7. Attacker: a person seeking to expose and/or exploit vulnerabilities.

LEGEND

1. **[C]** indicates that the component can have different levels of attack risk according to its configuration.
2. **[O]** indicates that the component requires configuration to be enabled.

INFRASTRUCTURE

Frontend

1. **Static assets** (i.e., Javascript, CSS, HTML, images)
    a. Files are embedded into the Distribution.
    b. File are served from Distribution.

2. **Cross-site Scripting**
    a. Content-Security-Policy Headers are not implemented.
        i. Planning implementation in future releases.
        ii. Risk factor: Low.
    b. HTTPS-Only cookies. **[O]**
        i. Codecov SSL Mode must be enabled.
    c. ALWAYS actively filters user submitted information.
    d. User input is accepted as Markdown, not HTML.
3. **Cookies**
    a. Stored in HTTPS-Only. **[O]**
    b. Tokens containing sensitive information are ALWAYS encrypted.
4. **Command Injection**
    a. User input is ALWAYS aggressively validated.

Backend

1. **OAuth Tokens**
    a. Tokens are ALWAYS encrypted using AES 256 bit encryption with multiple salts.
    b. Tokens are NEVER displayed in text format.
    c. Tokens are NEVER logged.
2. **Logging sensitive data**
    a. Sensitive data is ALWAYS actively filtered before logging.

Database: PostgreSQL

1. **Sensitive data is ALWAYS encrypted**
2. **Source code is NEVER stored in the database**
3. **Injecting SQL Commands**
    a. Risk: Low.
        i. User input is ALWAYS aggressively filtered.
4. **CLI Access**
    a. Risk: Low.
        i. ONLY Administrators can access PostgreSQL CLI.

Database: Redis

1. **Caching source code [C]**
    a. Reports pending processing MAY contain source code.
    b. Cache is ALWAYS deleted once a report is processed.
    c. Cache is ALWAYS deleted 24 hours after being generated.
    d. Risk: Low.

        i. ONLY Administrators can access Redis CLI.
2. **Storing sensitive user information**
    a. Risk: None. User data is NEVER stored in Redis.
3. **Injecting Redis commands**
    a. Risk: None.

Archive: Disk

Enabled by default. Codecov will archive Raw Uploads, and processed reports, to the disk or mounted NFS drive.

1. **Encoded file locations** [C]
    a. Files paths are ALWAYS encoded with unique information to prevent unauthorized access.
2. **Archived Reports [C]**
    a. Risk: None.
        i. Reports NEVER contain source code or sensitive information.
3. **Archived Raw Uploads [C]**
    a. Risk: Low.
        i. Only Administrators SHOULD have access to the Machine.
        ii. Archived Uploads MAY contain source code.

Archive: AWS

Disabled by default. If enabled, Codecov can archive reports to an AWS bucket.

1. **AWS is off-premise and public**
    a. Risk: Medium.
        i. An Attacker MUST know the AWS Bucket name and understand the encoded file naming structure in order to review the file.
        ii. An Attacker COULD access archived data without authorization.
2. **Encoded file locations** [C]
    b. Files paths are ALWAYS encoded with unique information to prevent unauthorized access.
4. **Archived Reports [C]**
    a. Risk: None.
        i. Reports NEVER contain source code or sensitive information.
5. **Archived Raw Uploads [C]**
    a. Archived Uploads **MAY** contain source code.
    b. Risk: Medium.
        i. An Attacker COULD discover the location of Uploads.

SUMMARY

OAuth Tokens and Archived Uploads are considered high-value targets for an Attacker. Codecov makes the best efforts to reduce the risk of exposing all sensitive information.

Please direct any questions or concerns to enterprise@codecov.io

Thank you and enjoy Codecov Enterprise.