Meethack Torino

Vulnerability Research & Exploit Development: GitLab - *CVE-2023-2825*

GitLab - CVE-2023-2825

Title	Severity
Arbitrary file read via uploads path traversal	critical

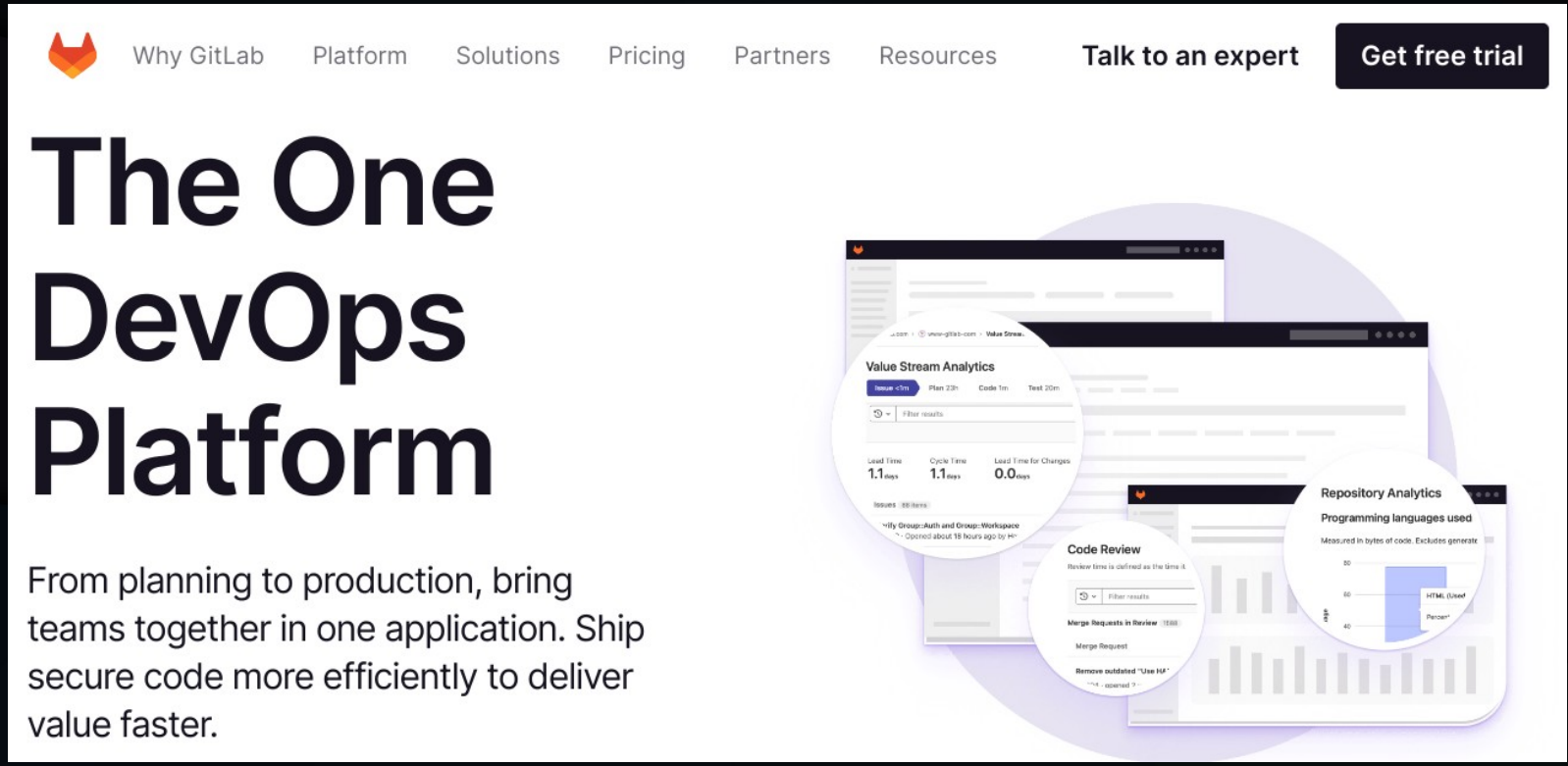
Arbitrary file read via uploads path traversal

An issue has been discovered in GitLab CE/EE affecting only version 16.0.0. An unauthenticated malicious user can use a path traversal vulnerability to read arbitrary files on the server when an attachment exists in a public project nested within at least five groups. This is a critical severity issue (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N`, 10.0). It is now mitigated in the latest release and is assigned CVE-2023-2825.

Thanks pwnie for reporting this vulnerability through our HackerOne bug bounty program.

https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/

What is GitLab?



https://about.gitlab.com/

Let’s try to “discover” the exploit blindly

- We can use:
  - Bulletin – https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/
  - Vulnerable container – gitlab/gitlab-ce:16.0.0-ce.0
  - Vulnerable source code – https://gitlab.com/gitlab-org/gitlab-foss/-/tree/v16.0.0/
  - Fixed source code – https://gitlab.com/gitlab-org/gitlab-foss/-/tree/v16.0.1/
- Let’s try not to use:
  - Public exploits/write-ups
    - https://labs.watchtowr.com/gitlab-arbitrary-file-read-gitlab-cve-2023-2825-analysis/
    - https://github.com/Occamsec/CVE-2023-2825
    - https://hackerone.com/reports/1994725 (not public, yet)

Local vulnerable environment

- Setup:
  - `export GITLAB_HOME=/srv/gitlab`
  - ```
    docker run --detach --rm \
      --hostname gitlab.example.com \
      --publish 443:443 --publish 80:80 --publish 22:22 \
      --name vuln-gitlab \
      --volume $GITLAB_HOME/config:/etc/gitlab \
      --volume $GITLAB_HOME/logs:/var/log/gitlab \
      --volume $GITLAB_HOME/data:/var/opt/gitlab \
      --shm-size 256m \
      gitlab/gitlab-ce:16.0.0-ce.0
    ```
  - It might take a while before the Docker container starts to respond to queries.
  - Connect to `http://localhost`
  - Sign in with the username `root` and the password from the following command:
    - `docker exec -it vuln-gitlab grep 'Password:' /etc/gitlab/initial_root_password`
- Tear down:
  - `docker stop vuln-gitlab`

https://docs.gitlab.com/ee/install/docker.html#install-gitlab-using-docker-engine
    ```