Source Code Security(github)

- Managing vulnerabilities in you project

  a) browsing security vulnerability in the github advisory db

  b) security alerts for vulnerable dependencies

  c) automated security updates

  d) update vulnerable dependencies in repository

  e) managing alerts for vulnerable dependencies in your organization

Source Code Security(github)

a) browsing security vulnerability in the github advisory db

It allows you to browse or search for vulnerabilities which affect open source projects on github

Link:

https://github.com/advisories.

Below sources are used for vulnerabilities by github

The National Vulnerability Database

A combination of machine learning and human review to detect vulnerabilities in public commits on GitHub

Security advisories on GitHub

FriendsOfPHP

Source Code Security(github)

b) security alerts for vulnerable dependencies

GitHub detects and alerts on vulnerable dependencies in public repositories by default. To receive security alerts for vulnerable dependencies in a private repository, an owner of or person with admin access to the repository must enable the dependency graph and security alerts in the repository.

c) Automated Security updates

You can enable or disable automated security updates for an individual repository.

Repository → security → automated security updates

https://help.github.com/en/github/managing-security-vulnerabilities/configuring-automated-security-updates

Source Code Security(github)

d) update vulnerable dependencies in repository

steps:

i) github → repository → security

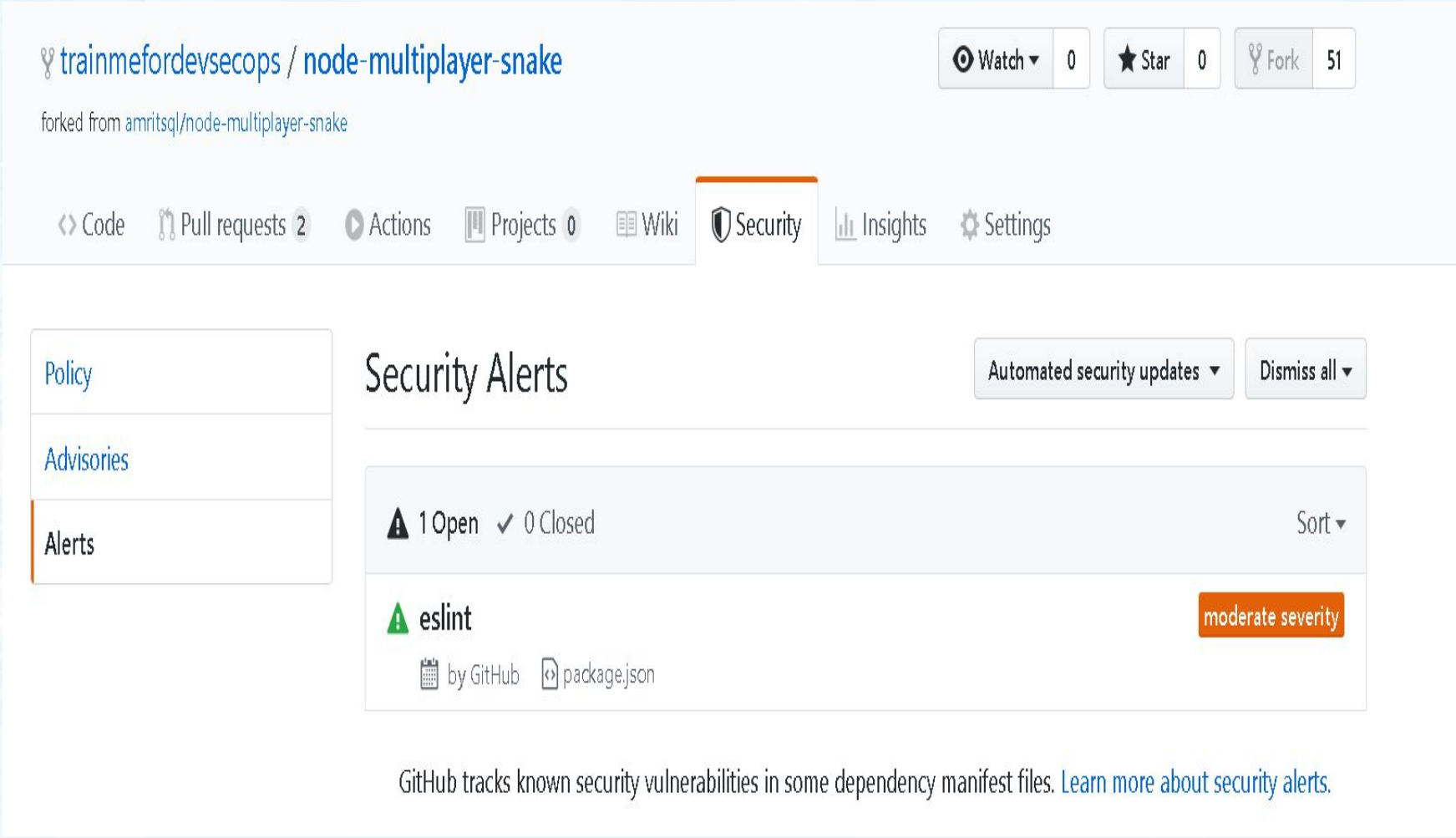
ii) click on the alert to view

iii) Review the details of the vulnerability and, if available, the pull request containing the automated security update.

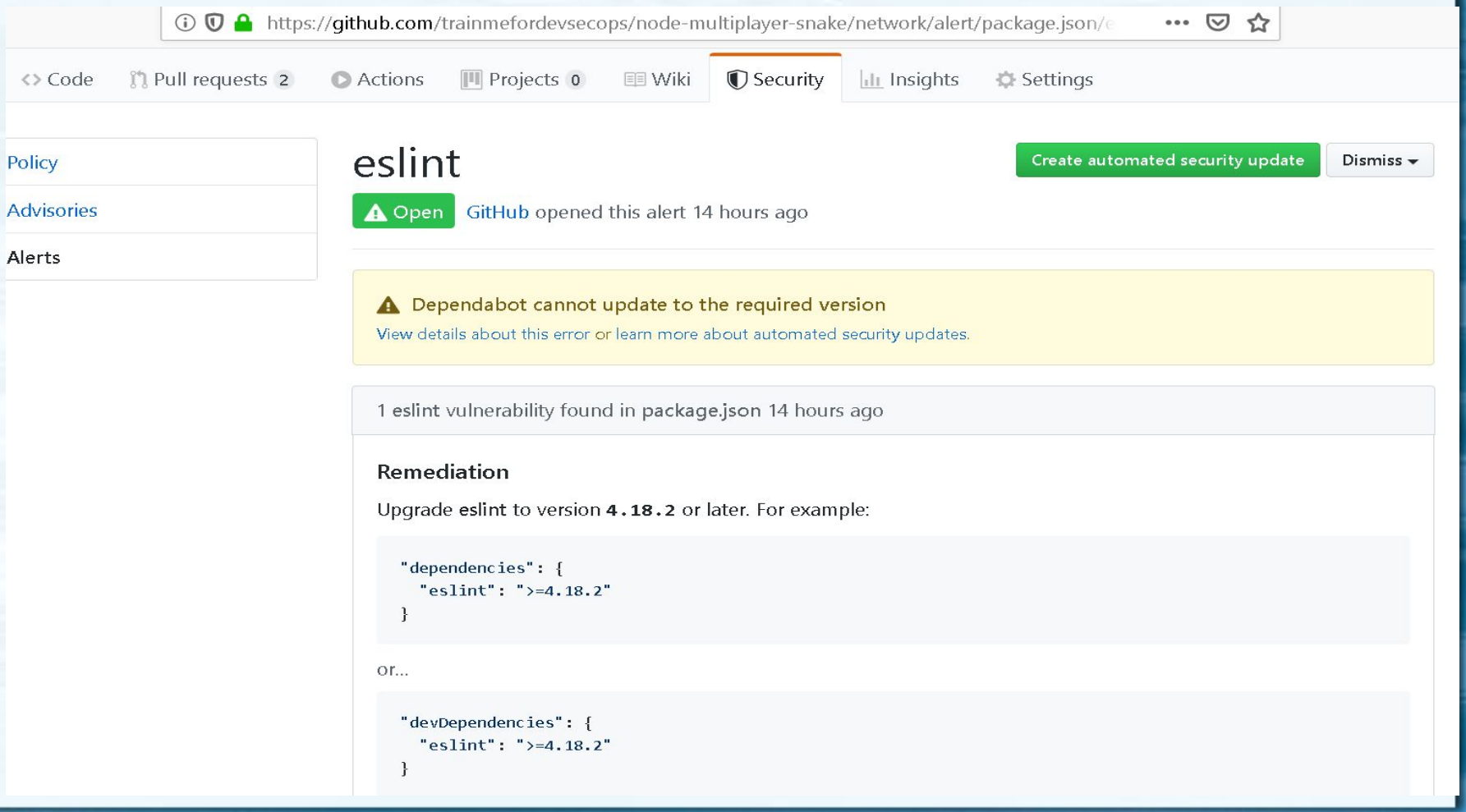
iv) if no security update for the alert, create a pull request to resolve the vulnerability

v) When you're ready to update your dependency and resolve the vulnerability, merge the pull request.

Source Code Security(github)

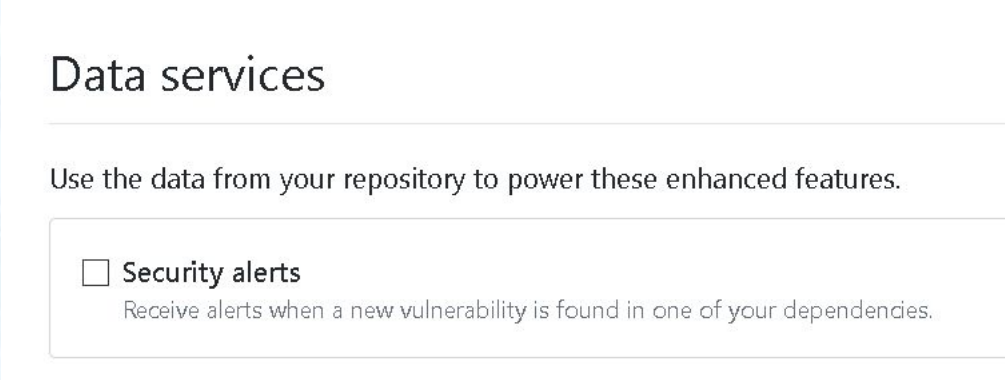


Source Code Security(github)



Source Code Security(github)

- e) managing alerts for vulnerable dependencies in your organization
- we can specify additional organization members or teams with write access to also receive security alerts for vulnerable dependencies.
- (I) On GitHub, navigate toe repository → settings
- (ii) click on the security tab
- (iii) check the checkbox security alerts under Data services as shown



Links & References

https://docs.github.com/en/code-security/security-overview/about-the-security-overview