

# Source Code Security(github)

- Managing vulnerabilities in your 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)

 trainmefordevsecops / node-multiplayer-snake

forked from amritsql/node-multiplayer-snake

 Watch ▾ 0

 Star 0

 Fork 51

 Code

 Pull requests 2

 Actions

 Projects 0

 Wiki

 Security

 Insights

 Settings

Policy

Advisories

Alerts

## Security Alerts

Automated security updates ▾

Dismiss all ▾

 1 Open ✓ 0 Closed

Sort ▾

 eslint

moderate severity

 by GitHub  package.json

GitHub tracks known security vulnerabilities in some dependency manifest files. [Learn more about security alerts.](#)

# Source Code Security(github)

Policy

Advisories

Alerts

eslint

Open

GitHub opened this alert 14 hours ago

⚠ Dependabot cannot update to the required version

[View details about this error](#) or [learn more about automated security updates](#).

1 eslint vulnerability found in package.json 14 hours ago

Remediation

Upgrade eslint to version **4.18.2** or later. For example:

```
"dependencies": {  
  "eslint": ">=4.18.2"  
}
```

or...

```
"devDependencies": {  
  "eslint": ">=4.18.2"  
}
```

Create automated security update

Dismiss



# 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 to repository → settings
- (ii) click on the security tab
- (iii) check the checkbox security alerts under Data services as shown

## Data services

Use the data from your repository to power these enhanced features.

☐ **Security alerts**

Receive alerts when a new vulnerability is found in one of your dependencies.

# Links & References

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