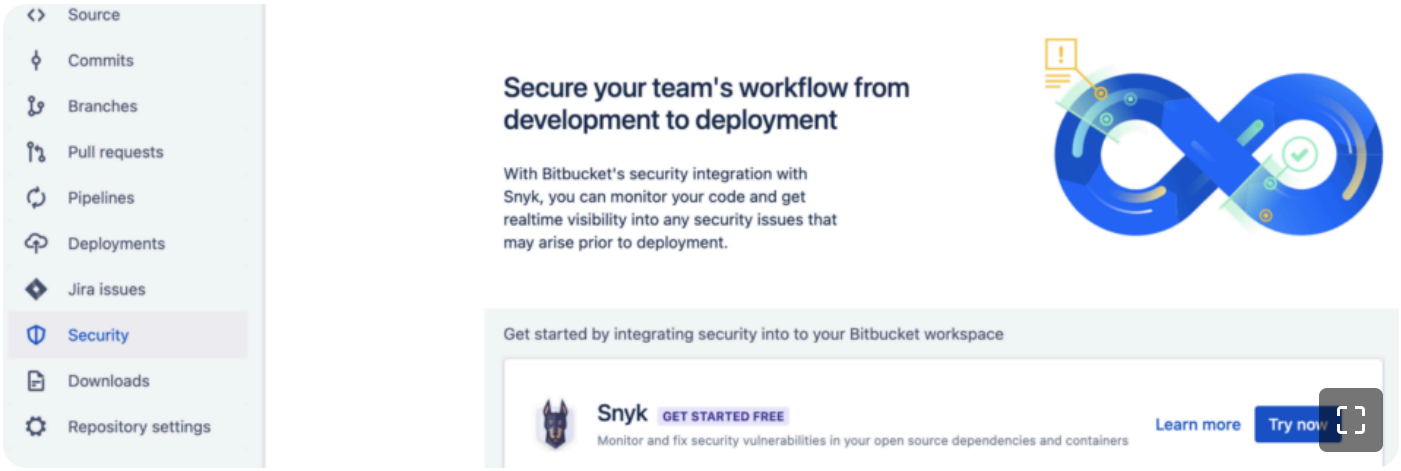
How to integrate security checks into your deployment workflow

September 22, 2021 BITBUCKET



As software applications grow in scale and complexity, the surface areas for security vulnerabilities and exploits grow with it.

Modern development practices include large amounts of code reuse. First, in the form of language-specific standard libraries such as the C++ STL, the Golang standard library, and Microsoft .NET. Second, in the form of open-source libraries found on places like Github. Much of this code is built using other libraries, introducing a web of dependencies into modern software.

This sheer amount of code leads to a high likelihood of security vulnerabilities being present. It's not possible to stay on top of vulnerabilities by manually checking all dependencies against CVE lists. Adding automated vulnerability scanning to CI/CD processes can help identify, and mitigate security risks.

Bitbucket has invested in a deeply embedded **native integration with Snyk**, the leading provider of security solutions for developers. This means no apps to install or configure. You can see details of security issues right within Bitbucket. Once you enable it, Snyk automatically checks your code and its dependencies and alerts you of vulnerabilities that are present so you can fix them before you deploy.

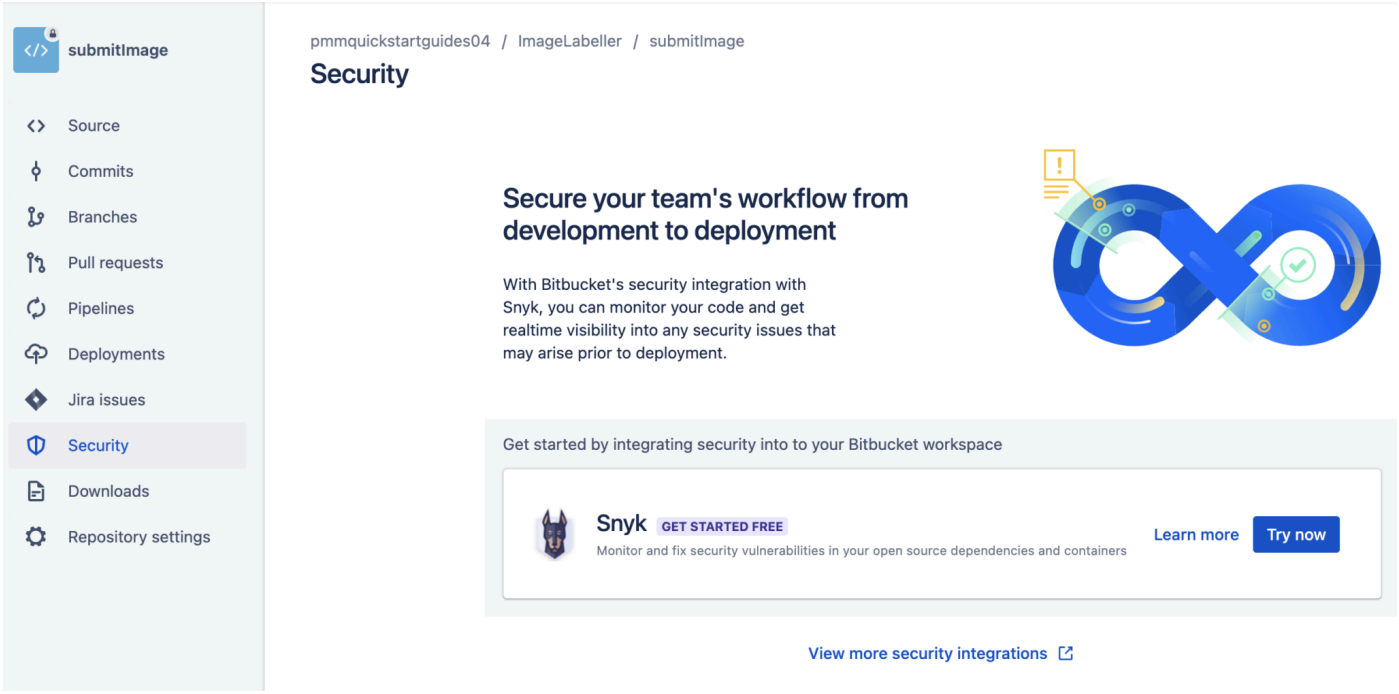
Snyk tracks 4x more vulnerabilities than any other commercial database and when new vulnerabilities are discovered, their database updates up to 46 days sooner than other databases.

Connecting Bitbucket and Snyk

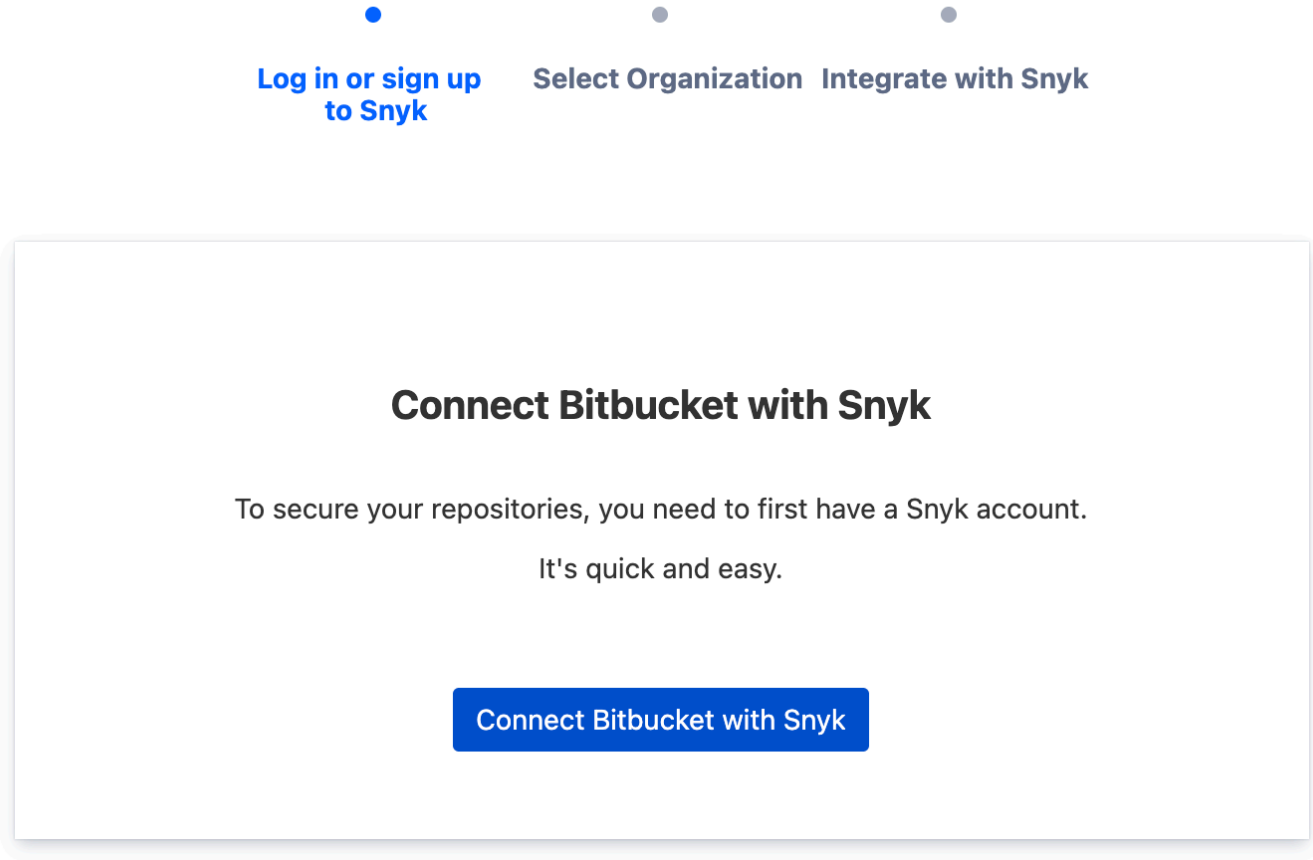
There are a couple of ways to work with Snyk in Bitbucket. The first is to enable the native Snyk integration to Bitbucket via the Security tab on your repository screen. The second is to add a Snyk step to a bitbucket-pipelines.yml file. There is no downside to doing both. The Synk integration in Bitbucket provides quick access to vulnerability data to anyone looking at the repository in Bitbucket. You can then click through to the Snyk website for additional information on each vulnerability found. The Snyk step in a bitbucket-pipelines.yml file enables automatic scanning on every commit in a pipeline.

Adding the Snyk integration to Bitbucket

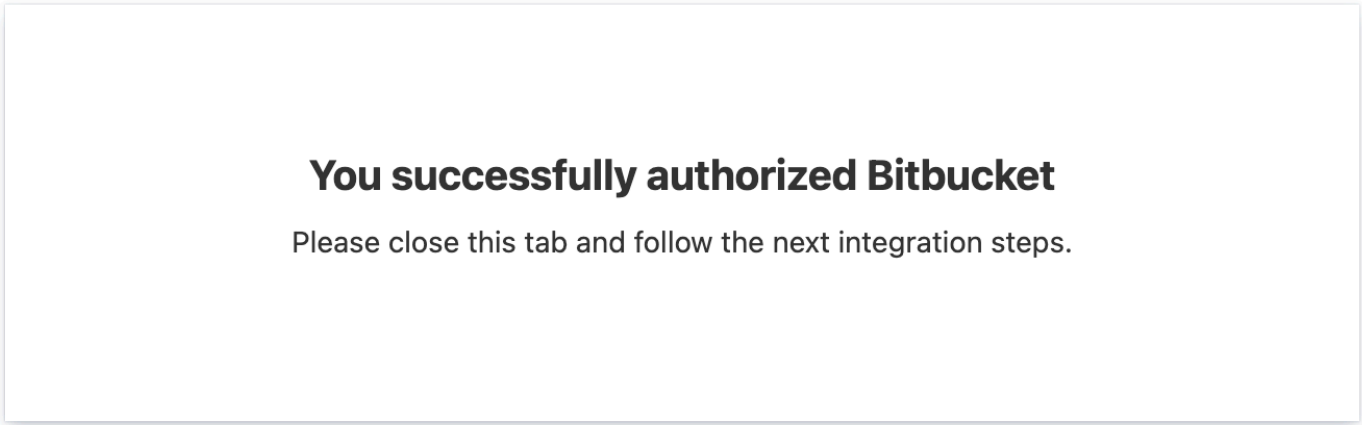
To add Snyk to a Bitbucket repository click on the **Security** tab, find the Snyk integration, then **Try now**.



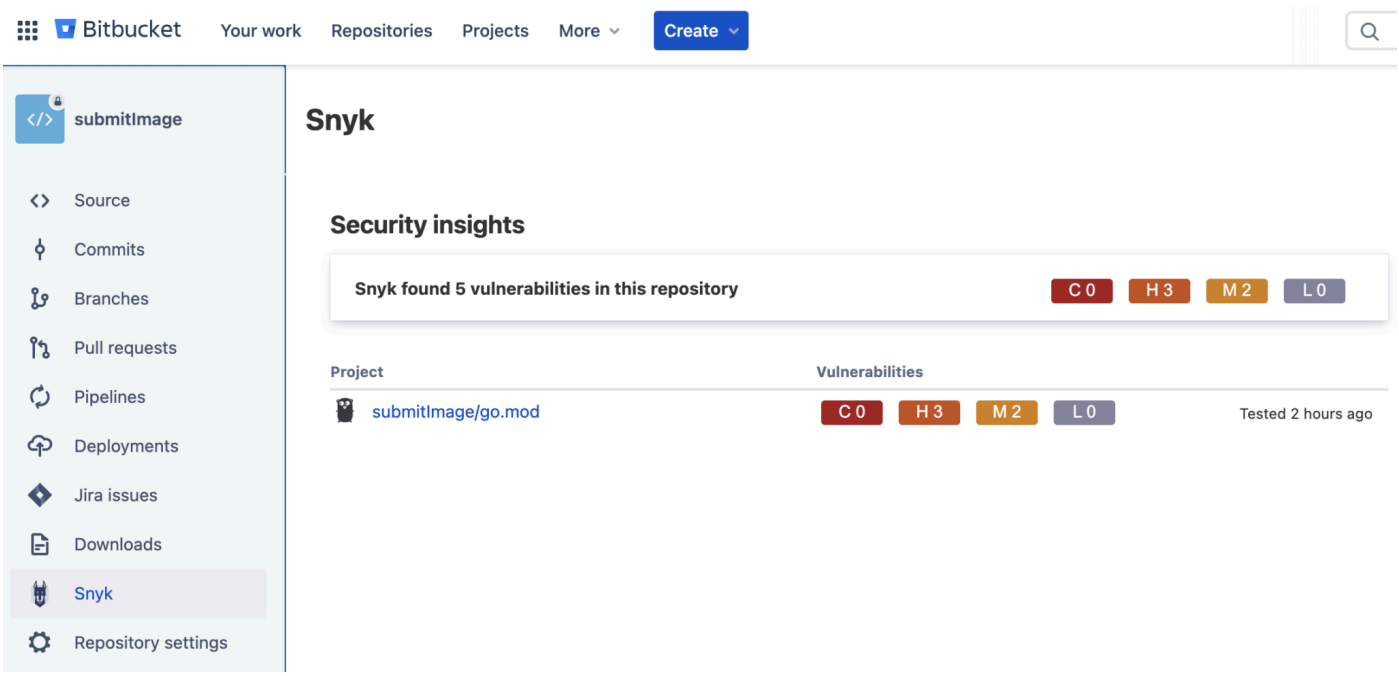
Grant access, and click **Connect Bitbucket with Snyk**.



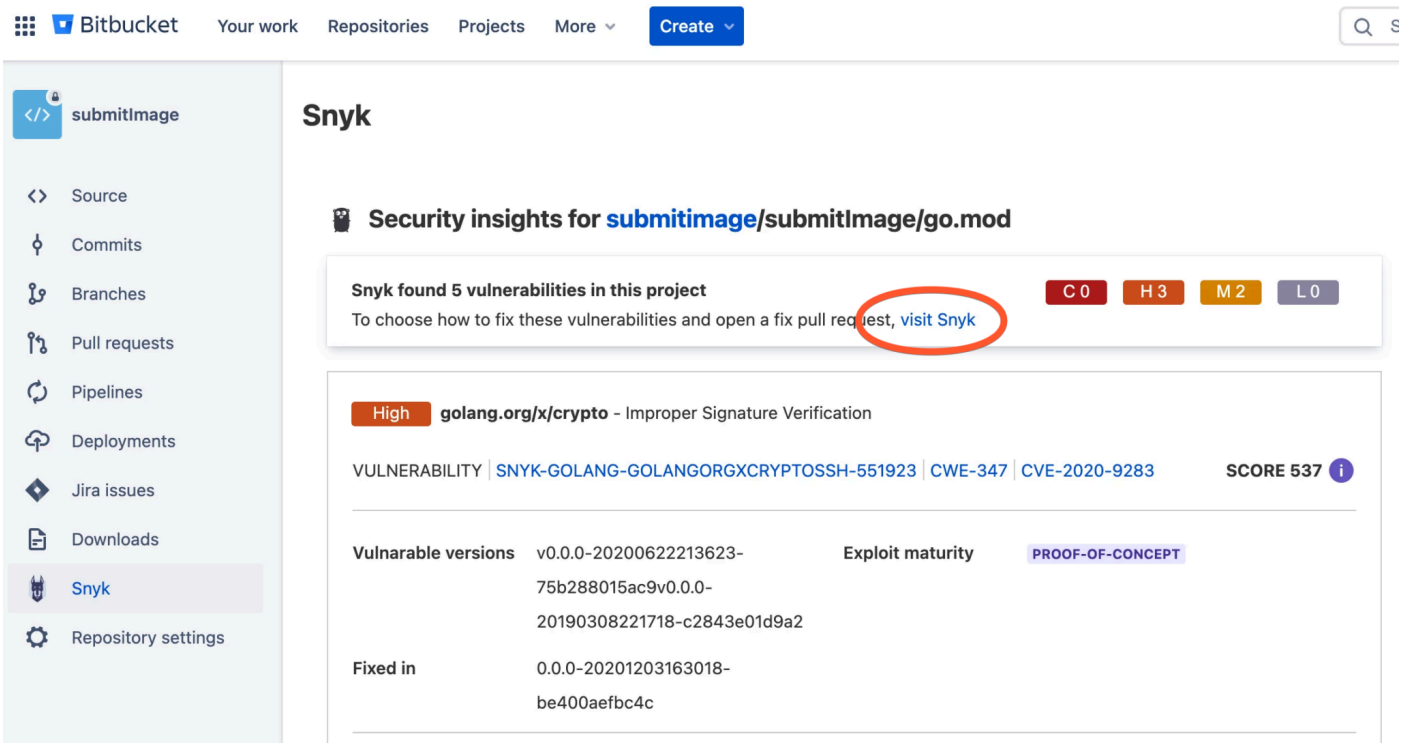
Once the integration is setup, close the tab.



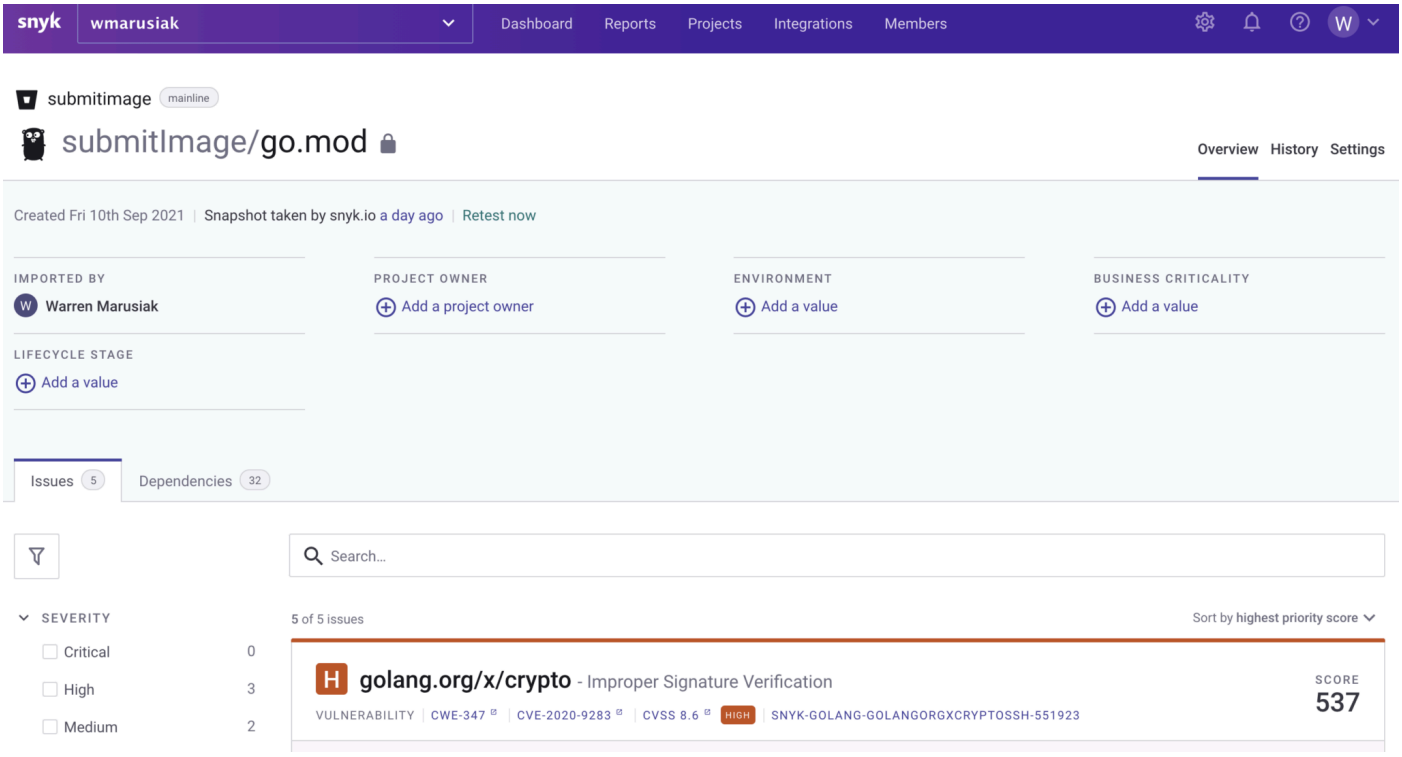
Click on the new **Snyk** option that appears in the left nav. Then click on the go.mod file to drill in to see more detailed information. The Golang repository uses go modules to manage dependencies in this example. For other kinds of repositories, there will be different dependency files.



To learn more about how to fix each vulnerability, click **visit Snyk** to go to the Snyk website.

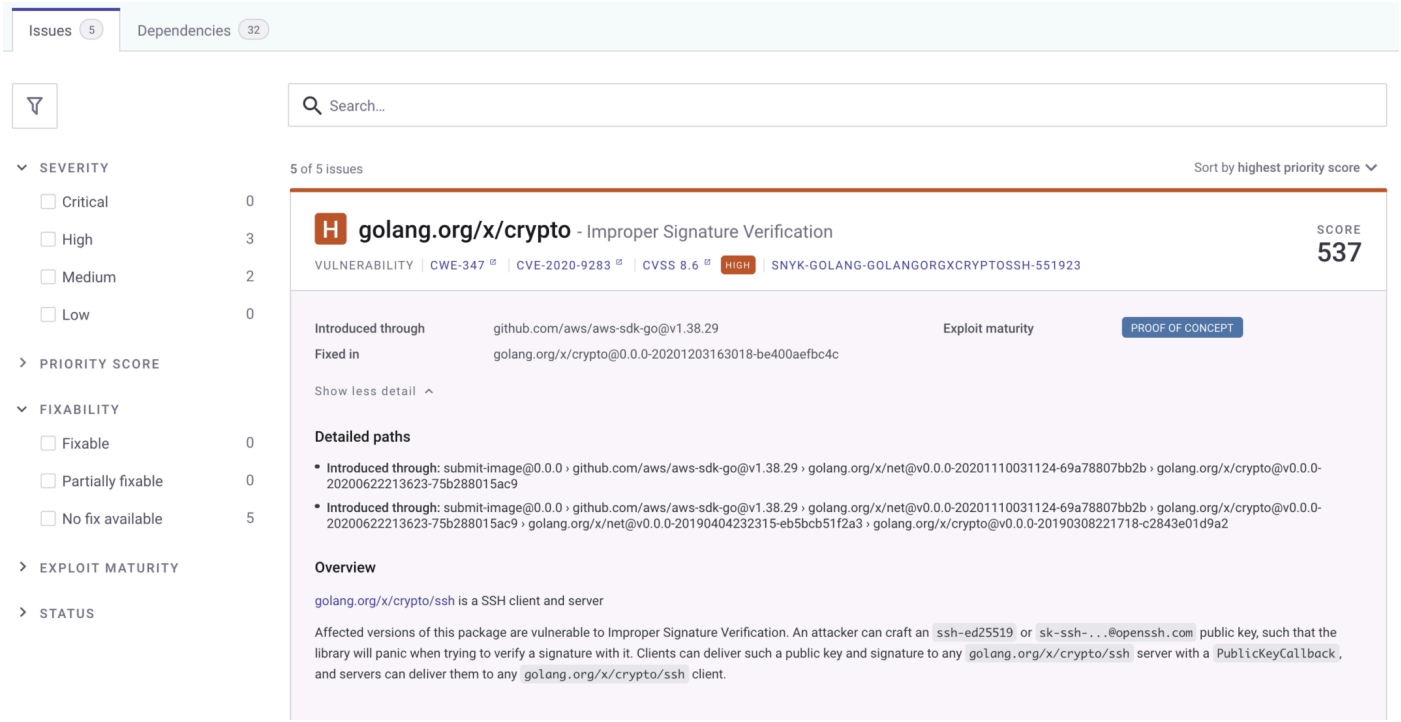


This view on the Snyk app is similar to the detail screen rendered in Bitbucket. This screen shows a list of vulnerabilities, along with additional information on each vulnerability.



Below is an example of a vulnerability report in Snyk. A hierarchy of where the vulnerability comes from is shown in the **Detailed paths** section. In the example below, you can see that SubmitImage inherits this vulnerability from the AWS Golang SDK. Snyk summarizes the status of all issues on the left. in this case, none of the issues are fixable. Notice there are

five **No fix available** issues under **Fixability**. This means that there is no current mitigation available for these issues. Developers can monitor the integration, and apply fixes as soon as they are available.



Add a Snyk step to bitbucket-pipelines.yml

In addition to accessing Snyk via the Bitbucket user interface, Snyk functionality can be accessed via Bitbucket pipelines by adding steps to bitbucket-pipelines.yml files. This means that vulnerability scanning will take place automatically on every commit and alert you of any security vulnerabilities.

Below are two bitbucket-pipelines.yml snippets for running Snyk tests as part of a pipeline.

Adding Snyk to Bitbucket pipelines for Golang

This example illustrates how to run **snyk test** for a Golang project using Go modules for dependency management.

```
definitions:
  steps:
    -step: &runsnyktest
        name: run snyk test
        image: snyk/snyk:golang
        script:
```

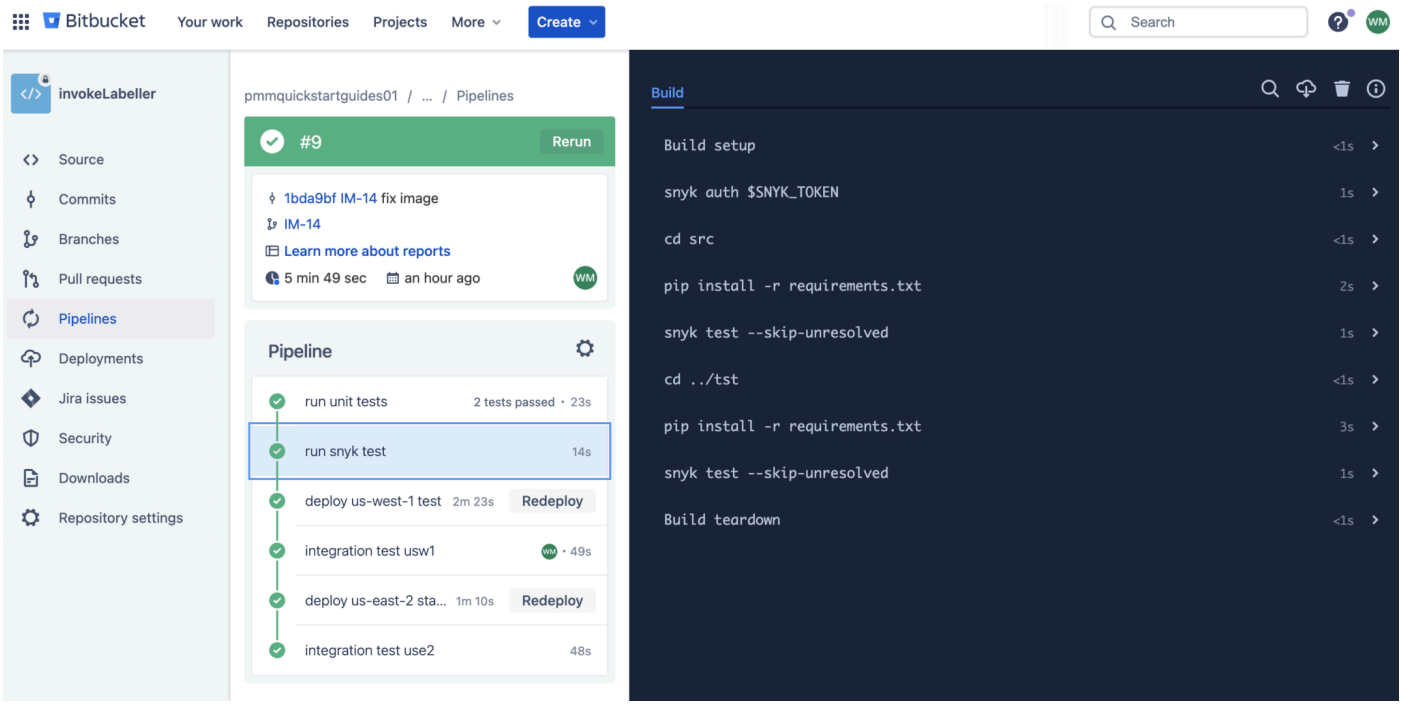
```
          - snyk auth $SNYK_TOKEN
          - cd submitImage
          - go mod graph
          - snyk test
pipelines:
  default:
    - step: *runsnyktest
```

Adding Snyk to Bitbucket pipelines for Python

This example illustrates how to run **snyk test** for a Python project using Pip for dependency management.

```
definitions:
  steps:
    -step: &runsnyktest
        name: run snyk test
        image: snyk/snyk:python
        script:
          - snyk auth $SNYK_TOKEN
          - cd src
          - snyk test --skip-unresolved
          - cd ../tst
          - snyk test --skip-unresolved
pipelines:
  default:
    - step: *runsnyktest
```

Here is what this looks like when the runsnyktest step is run in a Bitbucket pipeline.



Conclusion

The practice of integrating security into your CICD pipeline is a core tenet of DevSecOps. **DevSecOps** advocates that security should be applied to each phase of the typical **DevOps pipeline**: plan, code, build, test, release, and deploy. By incorporating security into your workflow, it becomes an active, integrated part of the development process vs an afterthought. This means safer apps, fewer incidents, and happier customers.

Related links:

- **DevSecOps tools**
- **DevSecOps tutorials**
- **Atlassian Open DevOps solution**

ABOUT THIS ARTICLE

WARREN MARUSIAK

Inside **Atlassian**

Get insights like this in your inbox

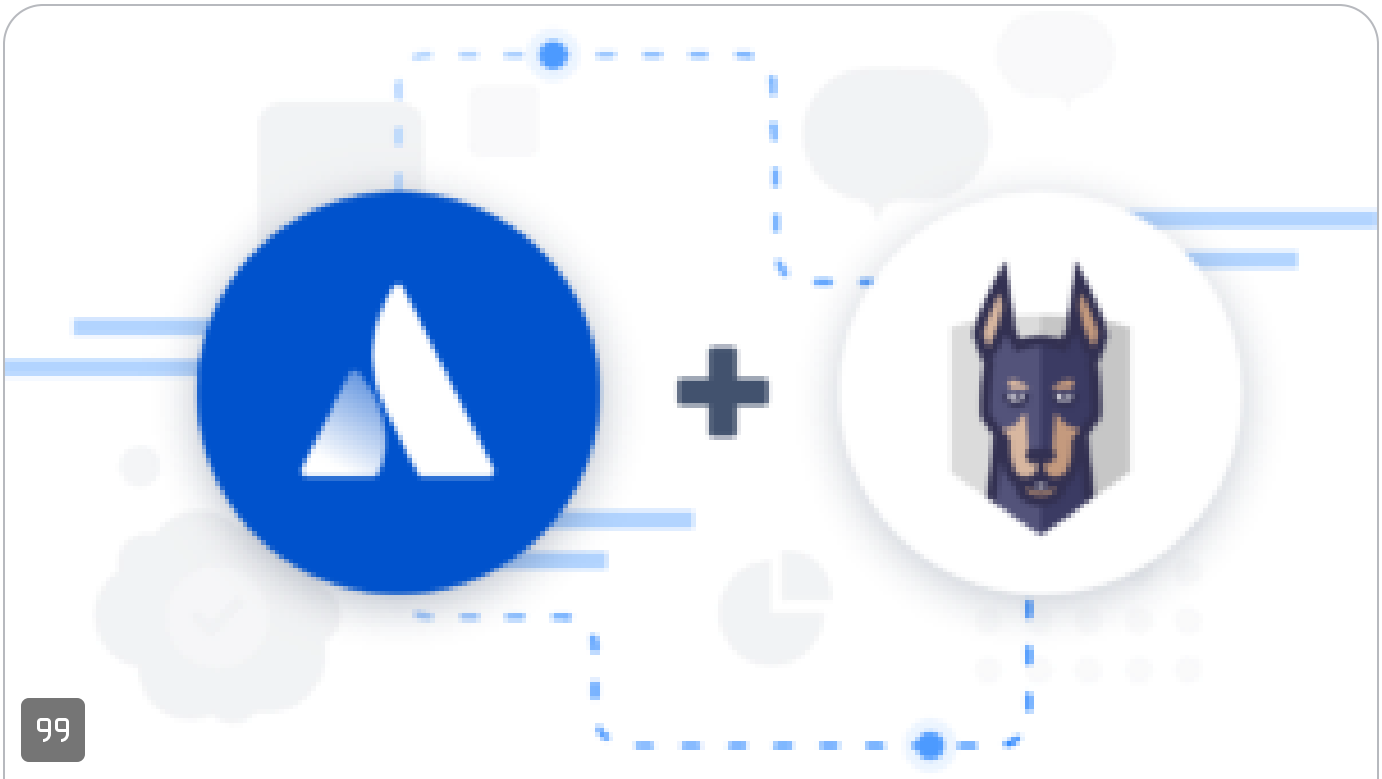
Sign up now

Related content

ARTICLE IN BITBUCKET

Keep your dependencies up-to-date with Snyk auto upgrade for Bitbucket Cloud

This article was written by Sarah Conway from Snyk, a company that helps organizations find and fix vulnerabilities in open source dependencies and container images. Keeping your dependencies up to date has a lot of value – it...



99

ARTICLE IN BITBUCKET

Integrate security into development with Snyk, now a seamless part of Bitbucket Cloud

Even small vulnerabilities can cost a team a lot. All too frequently we see news reports of organisations that mishandled their code & build level security, causing customer data to be exposed. The high publicity of these mistakes proves that...

ARTICLE IN BITBUCKET

Automate manual tasks with Bitbucket Pipelines

Each time you make changes to your code, you have to go through many manual steps like testing, building artifacts, deploying to several environments and more...

Resources

Technical support

Purchasing & licensing

Atlassian Community

Team Playbook

Knowledge base

Marketplace

My account

Create support ticket →

Learn

Partners

Training & certification

Documentation

Developer resources

Enterprise services

See all resources →