

How to integrate security checks into your deployment workflow

September 22, 2021 BITBUCKET

<>

Source

🔗

Commits

🌿

Branches

🔗

Pull requests

🔄

Pipelines

📦

Deployments

🔍

Jira issues

🛡️

Security

📄

Downloads

⚙️

Repository settings

Secure your team's workflow from development to deployment

With Bitbucket's security integration with Snyk, you can monitor your code and get realtime visibility into any security issues that may arise prior to deployment.

Get started by integrating security into to your Bitbucket workspace

 **Snyk** GET STARTED FREE

Monitor and fix security vulnerabilities in your open source dependencies and containers

Learn more

Try now



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 Snyk 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**.

</> submitImage

<> Source

Commits

Branches

Pull requests

Pipelines

Deployments

Jira issues

Security

Downloads

Repository settings

pmmquickstartguides04 / ImageLabeller / submitImage

Security

Secure your team's workflow from development to deployment

With Bitbucket's security integration with Snyk, you can monitor your code and get realtime visibility into any security issues that may arise prior to deployment.



Get started by integrating security into to your Bitbucket workspace

 **Snyk** GET STARTED FREE

Monitor and fix security vulnerabilities in your open source dependencies and containers

[Learn more](#) [Try now](#)

[View more security integrations](#)

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

Log in or sign up to Snyk

Select Organization

Integrate with Snyk

Connect Bitbucket with Snyk

To secure your repositories, you need to first have a Snyk account.

It's quick and easy.

Connect Bitbucket with Snyk

Once the integration is setup, close the tab.

You successfully authorized Bitbucket

Please close this tab and follow the next integration steps.

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.

The screenshot shows the Bitbucket web interface. At the top, there's a navigation bar with 'Bitbucket', 'Your work', 'Repositories', 'Projects', 'More', and a 'Create' button. A search bar is on the right. The left sidebar contains a list of navigation items: 'submitImage' (selected), 'Source', 'Commits', 'Branches', 'Pull requests', 'Pipelines', 'Deployments', 'Jira issues', 'Downloads', 'Snyk' (highlighted), and 'Repository settings'. The main content area is titled 'Snyk' and shows 'Security insights'. A summary box states 'Snyk found 5 vulnerabilities in this repository' with a breakdown: C 0, H 3, M 2, L 0. Below this is a table of vulnerabilities.

Project	Vulnerabilities	
submitImage/go.mod	C 0 H 3 M 2 L 0	Tested 2 hours ago

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

Bitbucket Your work Repositories Projects More Create

submitImage

- Source
- Commits
- Branches
- Pull requests
- Pipelines
- Deployments
- Jira issues
- Downloads
- Snyk**
- Repository settings

Snyk

Security insights for submitImage/submitImage/go.mod

Snyk found 5 vulnerabilities in this project

To choose how to fix these vulnerabilities and open a fix pull request, [visit Snyk](#)

C 0 H 3 M 2 L 0

High golang.org/x/crypto - Improper Signature Verification

VULNERABILITY | SNYK-GOLANG-GOLANGORGXCRYPTOSSH-551923 | CWE-347 | CVE-2020-9283 SCORE 537

Vulnerable versions	v0.0.0-20200622213623-75b288015ac9v0.0.0-20190308221718-c2843e01d9a2	Exploit maturity	PROOF-OF-CONCEPT
Fixed in	0.0.0-20201203163018-be400aefbc4c		

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.

snyk wmarusiak Dashboard Reports Projects Integrations Members

submitImage (mainline)

submitImage/go.mod Overview History Settings

Created Fri 10th Sep 2021 | Snapshot taken by snyk.io a day ago | Retest now

IMPORTED BY W Warren Marusiak	PROJECT OWNER + Add a project owner	ENVIRONMENT + Add a value	BUSINESS CRITICALITY + Add a value
----------------------------------	--	------------------------------	---------------------------------------

LIFECYCLE STAGE
+ Add a value

Issues 5 Dependencies 32

SEVERITY

- ☐ Critical 0
- ☐ High 3
- ☐ Medium 2

5 of 5 issues

Sort by highest priority score

H golang.org/x/crypto - Improper Signature Verification SCORE 537

VULNERABILITY | CWE-347 | CVE-2020-9283 | CVSS 8.6 | HIGH | SNYK-GOLANG-GOLANGORGXCRYPTOSSH-551923

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.

The screenshot displays the Snyk web interface for a vulnerability in `golang.org/x/crypto`. The interface includes a sidebar with filters for Severity (Critical, High, Medium, Low), Priority Score, Fixability (Fixable, Partially fixable, No fix available), Exploit Maturity, and Status. The main content area shows a search bar and a list of 5 issues. The selected issue is titled "golang.org/x/crypto - Improper Signature Verification" with a score of 537. It is categorized as a Vulnerability with CWE-347, CVE-2020-9283, and CVSS 8.6 (High). The issue was introduced through `github.com/aws/aws-sdk-go@v1.38.29` and fixed in `golang.org/x/crypto@0.0.0-20201203163018-be400aefbc4c`. The exploit maturity is marked as "PROOF OF CONCEPT". The detailed paths show the vulnerability was introduced through `submit-image@0.0.0`, `github.com/aws/aws-sdk-go@v1.38.29`, `golang.org/x/net@v0.0.0-20201110031124-69a78807bb2b`, and `golang.org/x/crypto@v0.0.0-20200622213623-75b288015ac9`. The overview section states that affected versions of this package are vulnerable to Improper Signature Verification, and an attacker can craft an `ssh-ed25519` or `sk-ssh-...@openssh.com` public key, such that the library will panic when trying to verify a signature with it. Clients can deliver such a public key and signature to any `golang.org/x/crypto/ssh` server with a `PublicKeyCallback`, and servers can deliver them to any `golang.org/x/crypto/ssh` client.

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.

The screenshot displays the Bitbucket Pipelines interface. On the left, a sidebar shows navigation options: Source, Commits, Branches, Pull requests, Pipelines (selected), Deployments, Jira issues, Security, Downloads, and Repository settings. The main area shows a pipeline run for 'pmmquickstartguides01' with a status of '#9' and a 'Rerun' button. The pipeline steps are listed with their durations and status: 'run unit tests' (2 tests passed, 23s), 'run snyk test' (14s, highlighted), 'deploy us-west-1 test' (2m 23s, Redeploy), 'integration test usw1' (49s), 'deploy us-east-2 sta...' (1m 10s, Redeploy), and 'integration test use2' (48s). To the right, a 'Build' window shows the terminal output for the 'run snyk test' step, including commands like 'snyk auth \$SNYK_TOKEN', 'cd src', 'pip install -r requirements.txt', 'snyk test --skip-unresolved', and 'cd ../tst'.

Conclusion

The practice of integrating security into your CI/CD 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](#)

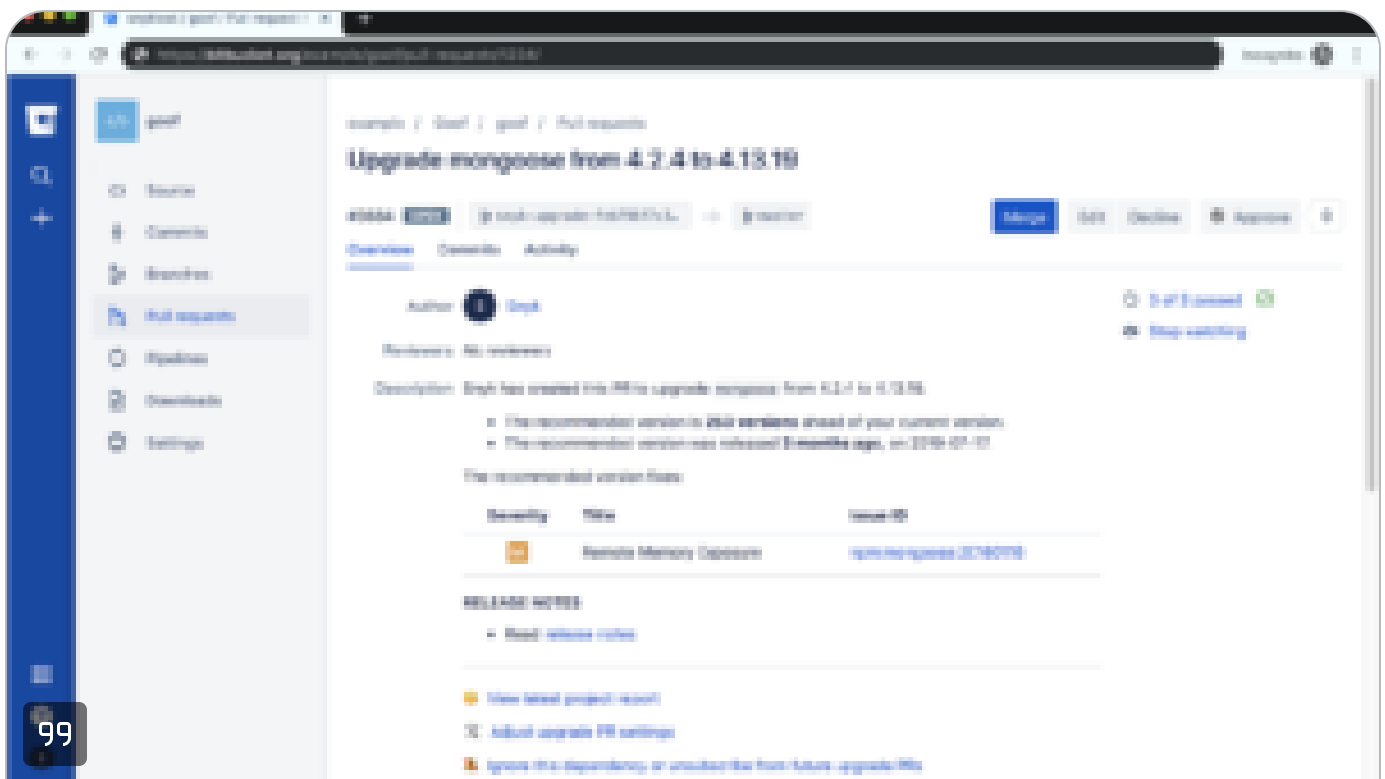
Subscribe for more

Inside Atlassian

Get insights like this in your inbox

Sign up now

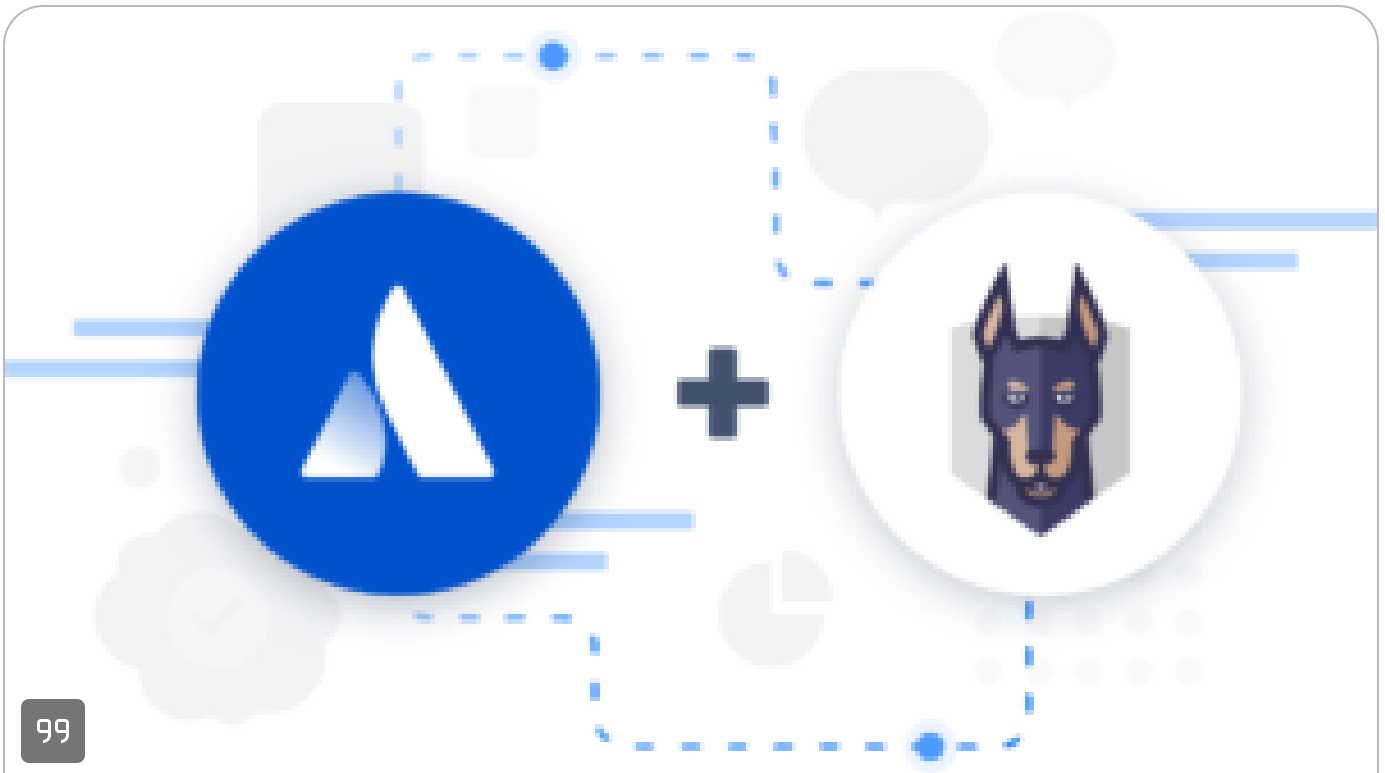
Related content



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...



99

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...



About the blog

Company

Careers

Events

Investor relations

Atlassian Foundation

Press kit

Contact us

Products

Rovo

Jira

Jira Align

Jira Service Management

Confluence

Loom

Trello

Bitbucket

See all products →

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 →

Copyright 2026 Atlassian

Privacy policy

Terms

Impressum

English