Command Injection

Affecting snyk-python-plugin package, versions **<1.24.2**

INTRODUCED: 29 SEP 2022 CVE-2022-22984 CWE-77 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `snyk-python-plugin` to version 1.24.2 or higher.

Overview

Affected versions of this package are vulnerable to Command Injection due to an incomplete fix for CVE-2022-40764.

A successful exploit allows attackers to run arbitrary commands on the host system where the Snyk CLI is installed by passing in crafted command line flags.

In order to exploit this vulnerability, a user would have to execute the `snyk test` command on untrusted files. In most cases, an attacker positioned to control the command line arguments to the Snyk CLI would already be positioned to execute arbitrary commands. However, this could be abused in specific scenarios, such as continuous integration pipelines, where developers can control the arguments passed to the Snyk CLI to leverage this component as part of a wider attack against an integration/build pipeline.

This issue has been addressed in the latest Snyk Docker images available at https://hub.docker.com/r/snyk/snyk as of 2022-11-29. Images downloaded and built prior to that date should be updated.

The issue has also been addressed in the Snyk TeamCity CI/CD plugin as of version v20221130.093605.

References

- GitHub Commit (CLI)
- GitHub Commit (snyk-cocoapods-plugin)
- GitHub Commit (snyk-docker-plugin)
- GitHub Commit (snyk-gradle-plugin)
- GitHub Commit (snyk-hex-plugin)
- GitHub Commit (snyk-mvn-plugin)
- GitHub Commit (snyk-python-plugin)
- GitHub Commit (snyk-sbt-plugin)
- Imperva Blog Post
- Snyk Blog Post

Snyk CVSS

5.0 MEDIUM

Exploit Maturity	Proof of concept
Attack Complexity	High

See more

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JS-SNYKPYTHONPLUGIN-3039677
Published	30 Nov 2022
Disclosed	29 Sep 2022
Credit	Ron Masas - Imperva

Report a new vulnerability | Found a mistake?

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Join the >> community

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.