snyk Vulnerability DB

Snyk Vulnerability Database > pip > cookiecutter

Command Injection

Affecting cookiecutter package, versions [,2.1.1)

INTRODUCED: 2 MAR 2022 CVE-2022-24065 Share Share

CWE-78 FIRST ADDED BY SNYK

How to fix?

Upgrade cookiecutter to version 2.1.1 or higher.

Overview

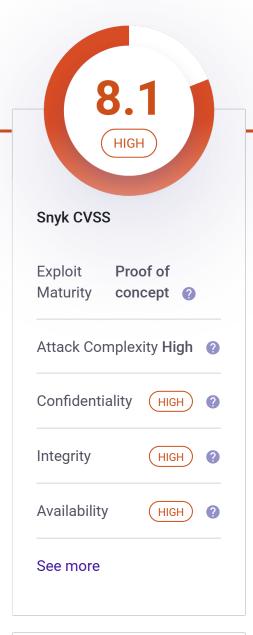
cookiecutter is a command-line utility that creates projects from cookiecutters.

Affected versions of this package are vulnerable to Command Injection via hg argument injection. When calling the cookiecutter function from Python code with the checkout parameter, it is passed to the hg checkout command in a way that additional flags can be set. The additional flags can be used to perform a command injection.

PoC

from cookiecutter.main import cookiecutter
checkout = "--config=alias.checkout=!touch
./HELLO" cookiecutter('some valid hg repository',
checkout=checkout)

Q Search by package n



> NVD 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what

References

- GitHub Commit
- GitHub Release

components are vulnerable in your application, and suggest you quick fixes.

Test your applications

SnykSNYK-PYTHON-ID COOKIECUTTER-2414281

Published 2 Jun 2022

Disclosed 2 Mar 2022

CreditAlessio Della Libera of Snyk Research Team

Report a new vulnerability

Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

Documentation	
Disclosed Vulnerabilities	
Blog	
FAQs	
COMPANY	
About	
Jobs	
Contact	
Policies	
Do Not Sell My Personal Information	
CONTACT US	
Support	
Report a new vuln	
Press Kit	
Events	
	FIND US ONLINE



TRACK OUR DEVELOPMENT

© 2022 Snyk Limited

RESOURCES

Vulnerability DB

Registered in England and Wales. Company number: 09677925

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