

Command Injection

Affecting [cookiecutter](#) package, versions [\[2.1.1\)](#)

INTRODUCED: 2 MAR 2022 [CVE-2022-24065](#) 

CWE-78 

FIRST ADDED BY SNYK

Share 

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)
```



Snyk CVSS

Exploit Maturity Proof of concept 

Attack Complexity High 

Confidentiality HIGH 

Integrity HIGH 

Availability HIGH 

[See more](#)

> **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](#)

application and see what 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

RESOURCES

[Vulnerability DB](#)

[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



Join the >>
community

© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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

