lirantal / **simple-git-command-injection.md** Secret

Created 8 months ago

Command Injection vulnerability in simple-git@3.4.0

simple-git-command-injection.md

Command Injection vulnerability in simple-git@3.4.0

`simple-git` describes itself as a lightweight interface for running git commands in any node.js application.

Resources:

- Project's GitHub source code: https://github.com/steveukx/git-js
- Project's npm package: https://www.npmjs.com/package/simple-git

`simple-git` receive just over 2.2 million downloads a week, so this vulnerability report should probably be timely.

Background on exploitation

I'm reporting a Command Injection vulnerability in `simple-git` npm package.

The vector of attack in this vulnerability was found to be possible after investigating prior Command Injection vulnerability report as described here https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-2421199 which only fixes the attack vector for the `git fetch` command.

However, a similar use of the `--upload-pack` feature of git is also supported for `git clone`, which the prior fix didn't cover.

New exploit

Install `simple-git@3.4.0` which is the latest.

Run the following code:

```
const simpleGit = require('simple-git')
const git2 = simpleGit()
git2.clone('file:///tmp/zero123', '/tmp/example-new-repo', ['--upload-pack=touch /tm
```

Observe a new file created: `/tmp/pwn`

Author

Liran Tal