Command Injection Vulnerability In Async-Git

NODE NODEJS JAVASCRIPT NPM RCE TYPESCRIPT

Adar Zandberg Jan 20, 2021

Details Overview

Summary

The `tag` and `reset` functions are exposed to a shell injection vulnerability.
Untrusted inputs containing metacharacters can potentially execute malicious code.

Product

async-git before 1.13.1

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

```
const git = require('async-git');
git.reset('; touch HACKED #')`
// or
git.tag('; touch HACKED #')
```

Expected Result:

A file named `HACKED` has been created

Remediation

Sanitize untrusted user input before passing it to one of the vulnerable functions or update async-git to version 1.13.1.

Credit

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

Resources

1. Commit af4c2aa