All vulnerability reports

Reflected cross-site scripting in vaadin-menu-bar webjar resources in Vaadin 14

Severity: Medium (Base score 6.1) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE entry: CVE-2021-33611

Overview

Missing output sanitization in test sources in `org.webjars.bowergithub.vaadin:vaadin-menu-bar` versions 1.0.0 through 1.2.0 (**Vaadin 14.0.0 through 14.4.4**) allows remote attackers to execute malicious JavaScript in browser by opening crafted URL.

See CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description

One of the test sources in `<vaadin-menu-bar>` web component contained a reflected XSS vulnerability. Tests for `<vaadin-menu-bar>` are not published in the npm registry (`@vaadin/vaadin-menu-bar`), but included in bower and, as a consequence, in `org.webjars.bowergithub.vaadin:vaadin-menu-bar` webjar. When web component webjars are accessible in the deployed Vaadin application, attacker can craft an URL, which, if opened in the browser by victim, will execute arbitrary JavaScript.

Web component webjar dependencies are only needed for legacy compatibility mode, and should be explicitly excluded in `pom.xml` when running in Vaadin 14 mode:

```
<dependency>
    <groupId>com.vaadin</groupId>
    <artifactId>vaadin</artifactId>
    <exclusions>
        <!-- Webjars are only needed when running in Vaadin 14 compatibility mode -->
        <exclusion>
            <groupId>com.vaadin.webjar</groupId>
            <artifactId>*</artifactId>
        </exclusion>
        <exclusion>
            <groupId>org.webjars.bowergithub.insites</groupId>
            <artifactId>*</artifactId>
        </exclusion>
        <exclusion>
            <groupId>org.webjars.bowergithub.polymer</groupId>
            <artifactId>*</artifactId>
        </exclusion>
        <exclusion>
            <groupId>org.webjars.bowergithub.polymerelements</groupId>
            <artifactId>*</artifactId>
        </exclusion>
        <exclusion>
            <groupId>org.webjars.bowergithub.vaadin</groupId>
            <artifactId>*</artifactId>
        </exclusion>
        <exclusion>
            <groupId>org.webjars.bowergithub.webcomponents</groupId>
            <artifactId>*</artifactId>
        </exclusion>
    </exclusions>
</dependency>
```

Affected products and mitigation

Users of affected versions should apply the following mitigation or upgrade. Releases that have fixed this issue include:

Product version	Mitigation
Vaadin 14.0.0 - 14.4.4	Upgrade to 14.4.5 or newer version

Artifacts

Maven coordinates	Vulnerable version	Fixed version
org.webjars.bowergithub.vaadin:vaadin-menu-bar	1.0.0 - 1.2.0	≥ 1.2.1

References

PR: https://github.com/vaadin/vaadin-menu-bar/pull/126

History

2021-11-01: Initial vulnerability report published

Company

About
Team
Careers
Contact
Brand

Platform

Flow
UI Components
Collaboration Kits
Acceleration Kits
DS Publisher
Designer
TestBench

Solutions

App creation
App modernization
Migration assistance
Design services
Vaadin support
Expert services

Developers

Developer portal
Start an app
Documentation
Add-on Directory
Training videos

Resources

Blog
Customer stories
Events & webinars
Platform FAQ
Framework comparison
For students

Community Terms Privacy Policy