

**Finding Name:** UserIconComponent Vulnerability

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Jaspriya Kaur | SCR | Senior Lead | Ontrack |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

The UserIconComponent is vulnerable due to insufficient input validation and reliance on external libraries like ts-md5 and D3.js. Inadequate validation of user data exposes the application to injection attacks. Dependency management issues pose risks of vulnerabilities or deprecated features. Proper input validation, dependency updates, and adherence to security best practices are necessary to mitigate these vulnerabilities and ensure application security.

**Risk Rating**

Impact: Major

Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

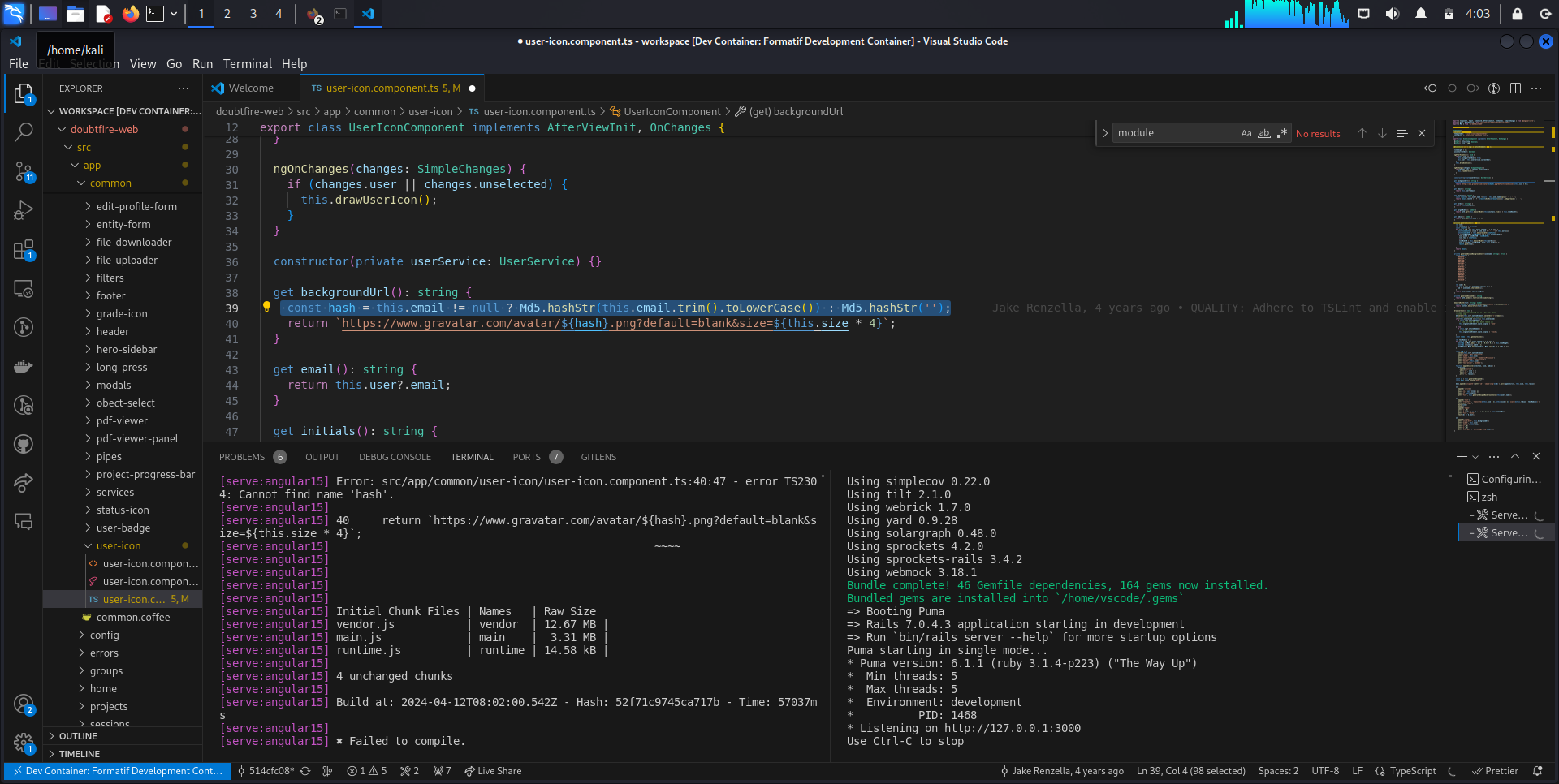
**Business Impact**

The vulnerability identified in the UserIconComponent could have a significant impact on the application's usability and security. This component is responsible for rendering user icons based on their email and name. However, a flaw in the implementation might lead to unexpected behavior or security risks, potentially affecting user experience and data integrity.

**Affected Assets**

The vulnerability affects the UserIconComponent within the application, potentially impacting any feature or functionality relying on user icons.

**Evidence**

**Step 1.** Navigate to the UserIconComponent within the application's codebase. ****

Path : /home/kali/doubtfire-deploy/doubtfire-web/src/app/common/user-icon/user-icon.component.ts

**Step 2.** Examine the drawUserIcon() method, which generates and renders the user icon.

**Step 3.** Note the usage of external libraries and potential dependencies, such as d3 and ts-md5.

**Step 4:** Analyze the logic for generating unique background colors and user initials.

**Step 5:** Review the implementation of SVG rendering and potential DOM manipulation.

**Remediation Advice**

To mitigate this vulnerability, consider the following steps:

drawUserIcon()

// if this.unselected is undefined or true

if (!this.unselected == null || this.unselected) {

if (this.svg?.nativeElement) {

// hide div from DOM (but don't remove it)

this.svg.nativeElement.style.display = 'none';

}

} else {

if (this.svg?.nativeElement) {

// add div to DOM

this.svg.nativeElement.style.display = 'block';

}

}

**To fix this: To fix this vulnerability, you can simplify the condition and handle the case when this. Unselected is undefined separately.**

// Handle the case when this.unselected is undefined

if (this.unselected === undefined) {

return;

}

// Hide or show the element based on this.unselected value

if (this.unselected) {

if (this.svg?.nativeElement) {

this.svg.nativeElement.style.display = 'none'; // Hide the element

}

} else {

if (this.svg?.nativeElement) {

this.svg.nativeElement.style.display = 'block'; // Show the element

}

}

**References**

* <https://angular.io/docs>
* <https://www.npmjs.com/package/ts-md5>
* <https://d3js.org/>
* <https://owasp.org/>
* <https://owasp.org/www-project-web-security-testing-guide/>

**Contact Details**

Add Name: Jaspriya Kaur

Email: s222196102@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.