

**Finding Name: Information Disclosure**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Natalia Khobotova | SCR | CSR Junior Lead | Ontrack |  |  |
|  |  |  |  |  |  |

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

**Finding Description**

The application is vulnerable to an Information Disclosure attack due to insufficient input validation and URI decoding. An attacker can craft specific malformed URI parameters to trigger a URIError, potentially exposing sensitive system details, error messages, or internal stack traces to the attacker.

**Risk Rating**  
Impact: Significant

Likelihood: High

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. |

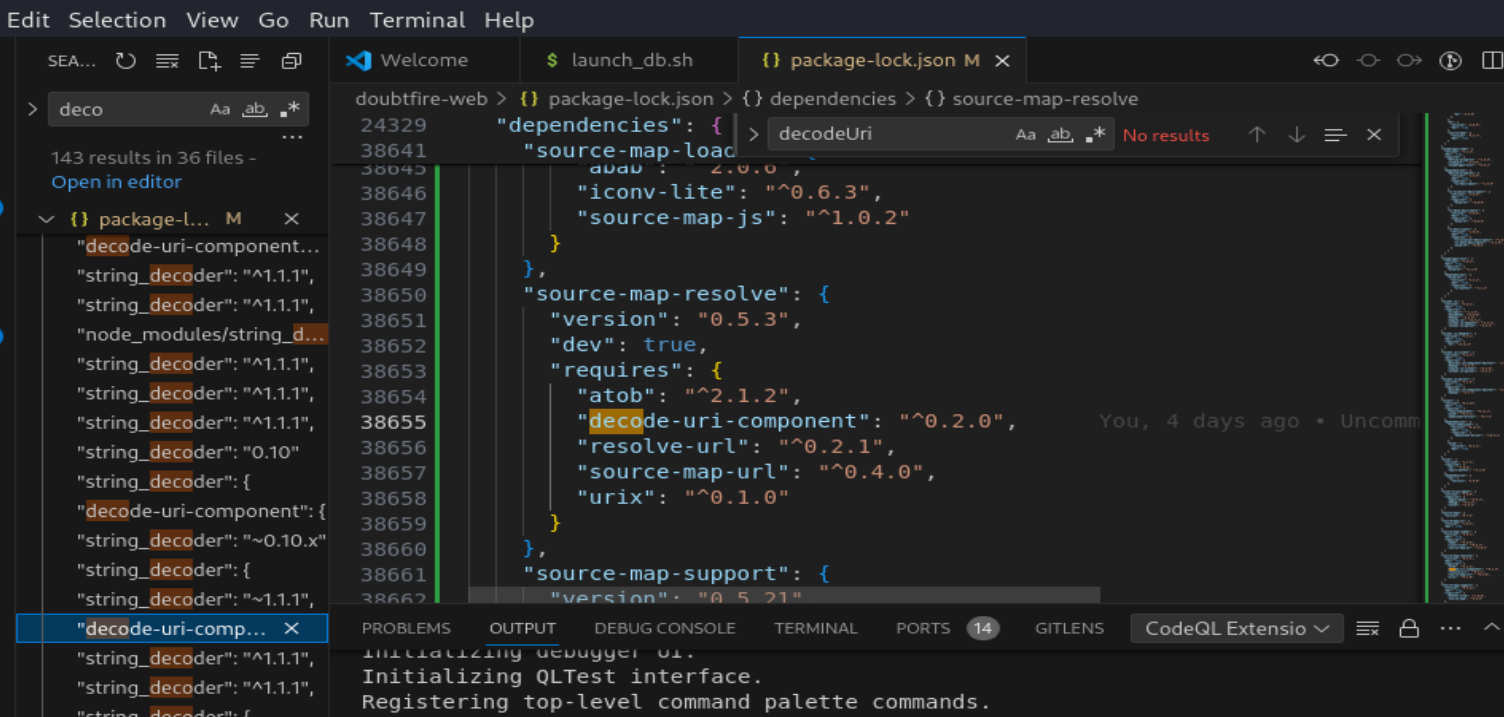
**Business Impact**

**Exposure of sensitive system details**: The attacker may gain access to sensitive information, error messages, or internal stack traces, which could be used to identify further vulnerabilities or weaknesses in the application.

**Reputation damage:** Exposing sensitive information or encountering frequent errors due to the vulnerability can negatively impact the company's reputation among users and stakeholders.

**Affected Assets**

* decode-uri-component package
* Application

**Evidence**Search for decode-url-component, it will bring the results with evidence that the package in in fact in use  
Navigate to the browser and append %ea%ba%5a%ba after localhost:4200/

A screenshot of a computer

Description automatically generated

**Remediation Advice**

Implement strict input validation mechanisms to validate and sanitise URI parameters before processing to ensure the application processes only valid and expected input.

Update the decode-uri-component package to the latest version, or the version where this vulnerability is addressed.

Implement proper error handling and logging mechanisms to handle malformed URI parameters gracefully without exposing sensitive system details, error messages, or internal stack traces to the attacker.

Implement security headers and response filtering to prevent sensitive information exposure through error messages, headers, or response bodies.

**References**

<https://security.snyk.io/vuln/SNYK-JS-DECODEURICOMPONENT-3149970>

[Information disclosure vulnerabilities | Web Security Academy (portswigger.net)](https://portswigger.net/web-security/information-disclosure#:~:text=How%20to%20prevent%20information%20disclosure%20vulnerabilities%201%20Make,are%20disabled%20in%20the%20production%20environment.%20More%20items)

[What Is an Information Disclosure Vulnerability? [Examples] (hackerone.com)](https://www.hackerone.com/vulnerability-management/information-disclosure-deep-dive)

**Contact Details**

• Natalia Khobotova

• s223011356@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.