

**Finding Name: Security and Dependency Upgrades: numpy, tornado, and Miscellaneous Updates**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Sharique Aizaz | PT | Project Member | Ontrack | Nabiha Masood |  |
|  |  |  |  |  |  |

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

**Finding Description**

The Denial of Service (DoS) vulnerability found in the rack gem affects versions >=1.3.0 to <2.2.8.1 and >=3.0.0 to <3.0.9.1. This vulnerability stems from inadequate handling of the Range request header. By meticulously creating Range headers, attackers can prompt the server to generate excessively large responses. Consequently, this could lead to resource exhaustion, rendering the system inaccessible to legitimate users. The vulnerability particularly impacts web applications utilizing the Rack::File middleware or the Rack::Utils.byte\_ranges methods, including those developed with Rails.

**Risk Rating**  
Impact: Significant  
Likelihood: Certain

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 Denial of Service (DoS) vulnerability in the rack gem could have significant business impacts. It may lead to service disruptions, damaging the company's reputation and customer trust. Legal and compliance issues may arise, resulting in potential fines. Poor customer experiences could lead to decreased loyalty and increased operational costs for mitigating the effects of the attack.

**Affected Assets**

The affected asset for the OnTrack web application, would be the web application itself. This includes all components and resources associated with the application, such as the application codebase, libraries, frameworks, databases, and any underlying infrastructure hosting the application. The security testing conducted by Snyk on this directory aims to identify vulnerabilities within the application's dependencies and components, ensuring the overall security and integrity of the OnTrack web application.

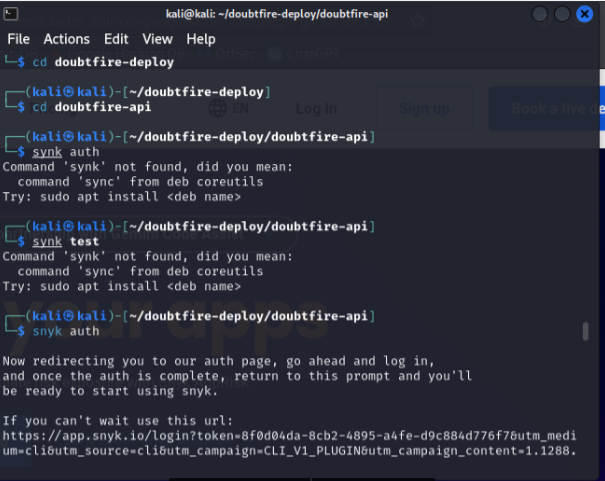
Impact:

The vulnerability could lead to a Denial of Service (DoS) condition, where attackers could exploit the flaw to overwhelm the server with excessive requests, resulting in downtime and service unavailability for legitimate users. This could have adverse effects on the availability and reliability of affected web applications.

**Evidence**

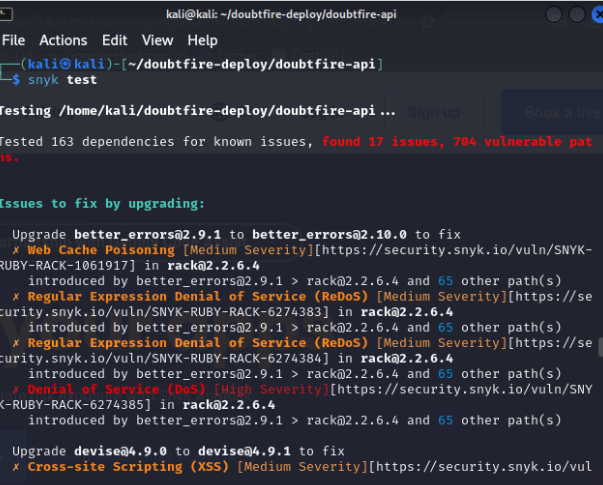
**Step 1.**

**Get into the directory where project is hosted and authenticate Snyk:**

****

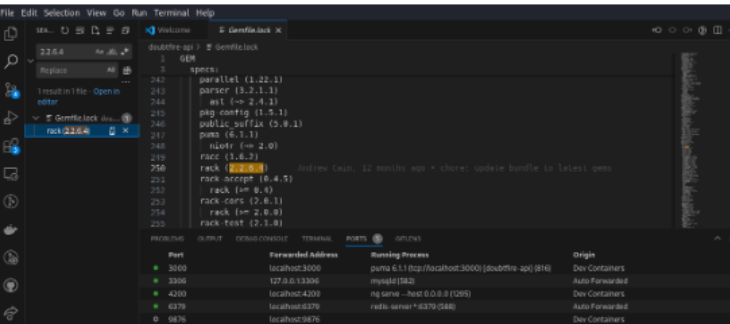
**Step 2.**

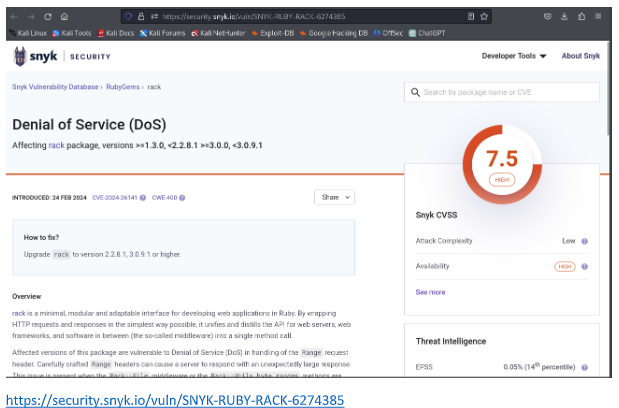
**After the auth is done run the scan, it list down all the possible issues and vulnerability.**

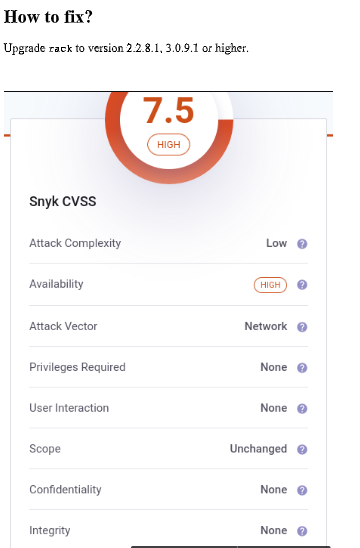
****

**Step 3.**

**As per the scan check the affected piece of code and also URL mentioned on CLI to get more detailed information of the Vulnerability and how to fix.**

****

****

****

**Remediation Advice**

To mitigate this vulnerability, it is strongly advised to upgrade the rack package to version 2.2.8.1 or 3.0.9.1 or higher. This update includes fixes to address the improper handling of Range request headers and helps prevent potential exploitation of the vulnerability. Additionally, developers should regularly monitor for security updates and promptly apply patches to ensure the security and stability of their applications.

**Update Dependencies**: It's essential to update the rack gem to a patched version (2.2.8.1 or 3.0.9.1 or higher) to mitigate the risk of exploitation in the future.

**Regular Security Audits**: Conduct regular security audits of your application's dependencies using tools like Snyk to identify and address any vulnerabilities proactively.

**Secure Configuration**: Ensure that your server and application are configured securely to mitigate the impact of potential DoS attacks. Implement rate limiting, request validation, and other security measures to protect against malicious requests.

**References**

Snyk

**Contact Details**

Sharique Aizaz – s223061215@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on