

**Finding Name:** Potential Dos Attack.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Gaurish Bhatia | SCR | Junior SCR team member | Ontrack | Jaspriya Kaur and Payas Paul |  |

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

**Finding Description**

A Denial of Service (DoS) attack refers to a category of attacks that are intended to render a system inaccessible to its legitimate users. In contrast to other security vulnerabilities, DoS attacks are not typically aimed at breaching security measures. Instead, their primary goal is to disrupt websites and services, causing them to become unavailable to genuine users and resulting in downtime.

**Risk Rating**  
Impact: Major  
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**

A Denial of service attack could lead to a temporary loss of services due to overloading amount of queries or processes, which could overpower the processing power of the server and could lead to shut down of services, which could further lead into loss of revenue.

**Affected Assets**

**Rack package version 2.2.6.4**

**Rack Package**

**Evidence**

The following screenshot shows the line of the vulnerable code :

**A screenshot of a computer

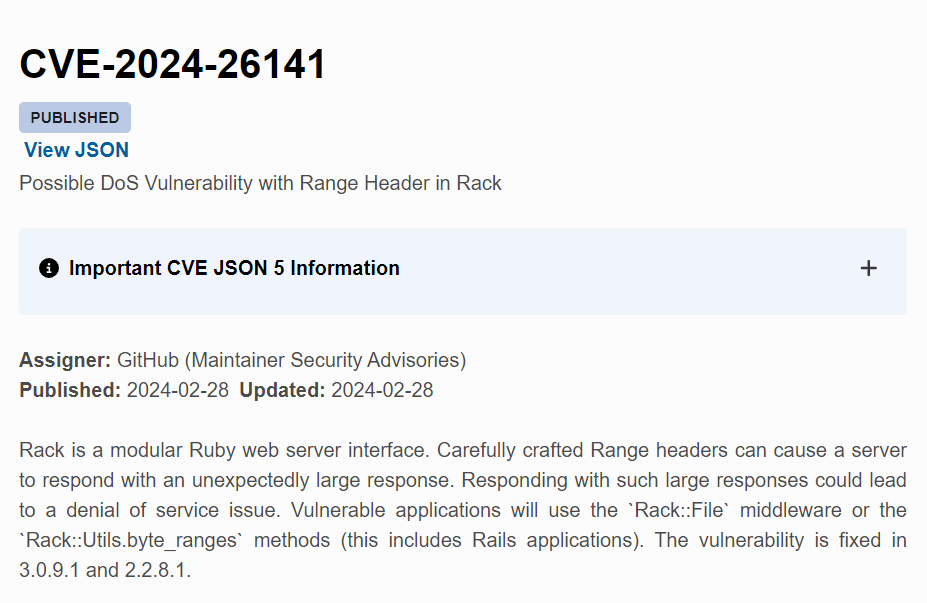
Description automatically generated**

**As it could be seen that the rack package is version 2.2.6.4, which is has CVE-2024-26141 and CWE-400 vulnerabilities, due to which there is potential Denial of service attack, which could be executed.**

**Here are the other evidence on the given vulnerability:**

**A screenshot of a computer

Description automatically generated**

****

**Remediation Advice**

This vulnerability could be fixed by upgrading to the version 2.2.8.1,3.0.9.1 or higher in order to mitigate the risk.

**References**

[**https://www.cve.org/CVERecord?id=CVE-2024-26141**](https://www.cve.org/CVERecord?id=CVE-2024-26141)

[**https://security.snyk.io/vuln/SNYK-RUBY-RACK-6274385**](https://security.snyk.io/vuln/SNYK-RUBY-RACK-6274385)

[**https://cwe.mitre.org/data/definitions/400.html**](https://cwe.mitre.org/data/definitions/400.html)

**Contact Details**

Gaurish Bhatia

S2221987151@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.