

**Finding Name: vulnerability in version of lodash**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Byeongnam Choe | SCR | Project Member | Ontrack | Nabiha Masood and Oliver Power |  |
|  |  |  |  |  |  |

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

**Finding Description**

The "lodash" library is a modern JavaScript utility library that offers modularity, performance, and extra features, and it is being used in the Ontrack app. However, the version of "lodash" currently being utilized is vulnerable to "command injection" (CVE-2021-23337) due to its default behavior, which could be exploited via templates.

**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**

This vulnerability could allow a threat actor to access and take advantage of the system, leveraging it against administrators and the business. They could manipulate the database, execute privilege escalation, achieve remote code execution, or compromise the entire system. Such breaches could severely damage the company's reputation and have a serious impact on both users and the company itself. Moreover, rectifying and maintaining service integrity would require significant financial investment

**Affected Assets**

User information

Web application

**Evidence**

Provide a step by step guide on how to reproduce the vulnerability with screenshots

**Step 1. A screenshot of a computer

Description automatically generated**

**I ran snyk against the app and discovered vulnerabilities.**

**Step 2. A screenshot of a computer

Description automatically generated**

**I discovered that the “Lodash” packages being used in the Ontrack app, along with their current versions, could potentially lead to exploitation in the future.**

**Step 3.**

A screenshot of a computer

Description automatically generated A screenshot of a computer screen

Description automatically generated

I double checked the version of lodash.

**Remediation Advice**

Update to version to 4.17.21 or higher

**References**

Snyk (monitoring tool)

https://security.snyk.io/vuln/SNYK-JS-LODASH-1040724

**Contact Details**

Byeongnam Choe (s222106547@deakin.edu.au)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.