

**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 ActionPack is one of the packages being used in the Ontrack app. The version of ActionPack being utilized is vulnerable to "Exposure of Data Element to Wrong Session (CVE-2024-26144)" due to the default behavior of sending the cookie header along with the user's session cookie. If an attacker exploits this vulnerability, it could lead to a leakage of user information.

**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**

If an attacker exploits this vulnerability, they could gain access to a user's session, potentially leading to the leakage of their information. This could severely damage the business's reputation, as they were unable to prevent such an incident, resulting in financial losses. Resources would need to be invested to fix this issue.

**Affected Assets**

User information

**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 ActionPack 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

I double checked the version of ActionPack.

**Remediation Advice**

Update to latest version

**References**

Synk.io

<https://security.snyk.io/vuln/SNYK-RUBY-ACTIONPACK-6274388>

**Contact Details**

Byeongnam Choe (s222106547@deakin.edu.au)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.