

**Finding Name:** Exposure of data element to wrong session.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Payas Paul | SCR | Senior Lead | Ontrack | Jaspriya Kaur |  |
|  |  |  |  |  |  |

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

**Finding Description**

The "Exposure of Data Element to Wrong Session" vulnerability in ActionPack, tracked as CVE-2024-26144, is a high severity vulnerability. It occurs due to the default behavior of sending a Set-Cookie header along with the user's session cookie when serving blobs and setting Cache-Control to public. Certain proxies may cache the Set-Cookie header, leading to an information leak. This vulnerability could allow an attacker to cause users to share sessions, potentially leading to unauthorized access to sensitive information.

**Risk Rating**  
Impact: Significant   
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**

1. Denial of Service (DoS) Vulnerability:
   * The CVE-2023-26141 vulnerability in the sidekiq package could allow an attacker to cause a DoS condition by manipulating the localStorage value.
   * A successful DoS attack could disrupt the availability of the affected systems and services, leading to downtime, loss of productivity, and potential reputational damage.
2. Potential Data Exposure:
   * The vulnerability is described as an "Exposure of Data Element to Wrong Session" issue, which could result in the leakage of sensitive user session information.
   * Data exposure incidents can have severe consequences, including the compromise of user accounts, theft of confidential data, and regulatory compliance issues (e.g., GDPR, HIPAA).
3. Exploitation and Public Disclosure:
   * The search results indicate that the vulnerability has been publicly disclosed, meaning that details about the issue are available to potential attackers.
   * The availability of exploit information increases the risk of the vulnerability being actively exploited, which could lead to further data breaches, system compromises, and financial losses.
4. Potential Cascading Effects:
   * If the vulnerable sidekiq package is used in other applications or systems, the impact of the vulnerability could extend beyond the initial affected component.
   * This could result in a wider security breach, affecting multiple systems and potentially exposing additional sensitive data or resources.

**Affected Assets**

1. Versions of the package sidekiq before 7.1.3.

The vulnerability description states that "Versions of the package sidekiq before 7.1.3 are vulnerable to Denial of Service (DoS) due to insufficient checks in the dashboard-charts.js file."This indicates that the vulnerable component is the sidekiq package, specifically versions prior to 7.1.3. An attacker can exploit this vulnerability by manipulating the localStorage value, which will cause excessive polling requests and lead to a Denial of Service (DoS) condition.

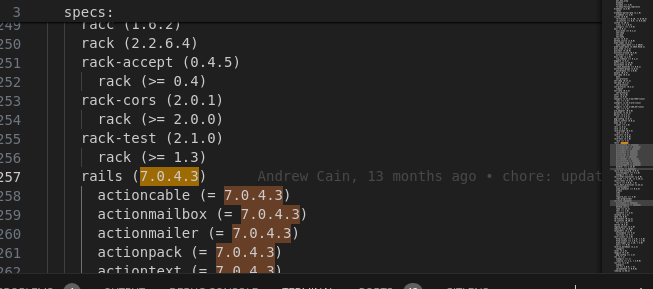
**Evidence**

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

**Step 1.**

**Go to doubtfire-deploy/doubtfire-api/Gemfile.lock - Line 257**

**Step 2.**

****

**Remediation Advice**

**The following steps can be taken to fix this issue.**

* Upgrade the affected package to a version that resolves the "Exposure of Data Element to Wrong Session" issue.
* Change the default behavior to prevent sending a Set-Cookie header along with the user's session cookie when serving blobs.
* Set Cache-Control to private to avoid potential information leakage.
* Ensure proxies do not cache the Set-Cookie header to prevent unintended sharing of the session.
* Promptly apply the available patch or upgrade to the affected sidekiq package to address the vulnerability.
* Assess the potential impact on any other systems or applications that may be using the vulnerable package.
* Review and strengthen security controls, such as network segmentation, access management, and monitoring, to detect and respond to any potential exploitation attempts.

**References**

**online tutorials** - <https://github.com/github/securitylab/issues/329>

**OWASP: The Open Web Application Security Project (OWASP) provides detailed information about session fixation, including examples and mitigation techniques. You can find more information on the OWASP website: OWASP Session Fixation.** [**https://owasp.org/www-community/attacks/Session\_fixation**](https://owasp.org/www-community/attacks/Session_fixation)

**PortSwigger: PortSwigger's Web Security Academy has a section on session fixation, which explains the vulnerability Session Fixation.** [**https://portswigger.net/support/using-burp-to-attack-session-management**](https://portswigger.net/support/using-burp-to-attack-session-management)

**Contact Details**

Payas Paul

612payaspaul@gmail.com

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.