

**Finding Name:** Cross Site Scripting(xss)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Gaurish Bhatia | SCR | SCR team member | Ontrack | Natalia Khobotova | NO |

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

**Finding Description**

Cross-site scripting (XSS) is a security hole in websites that lets attackers inject malicious scripts. These scripts run in users' browsers, potentially stealing data like cookies or passwords, or tricking users into giving away personal information. XSS attacks are common and can be hidden in many places on a website, like search bars or comments. Website owners need to be careful about handling user input to prevent XSS.

**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**

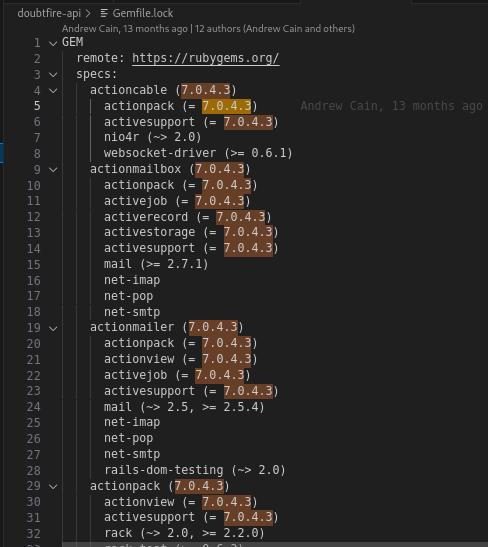
The XSS attacks could lead to a major impact on the business , which includes stolen user data, which might lead to a loss of trust from the user. The data stolen could be leaked by the attacker, which could lead to legal repercussions. At last, it will lead to loss in revenue to the company.

**Affected Assets**

The affected assets include the Ontrack server, the user data and the browser of the user, which will run the script injected by the user leading to steal in the user data.

**Evidence**

The following screenshot shows the line of the vulnerable code :

****

The affected file is doubtfire-deploy/doubtfire-api/gemfile.lock/actionpack.

As it could be seen on line 4, the action pack version is 7.0.4.3, which has cve-2023-28362 and CWE-79 vulnerabilities.

The following screenshots show the details on the same:

A screenshot of a computer

Description automatically generated

**A screenshot of a computer

Description automatically generated**

**Remediation Advice**

The vulnerability could be mitigated by upgrading the action pack to version 6.1.7.4,7.0.5.1 or higher.

**References**

[**https://cwe.mitre.org/data/definitions/79.html**](https://cwe.mitre.org/data/definitions/79.html)

[**https://security.snyk.io/vuln/SNYK-RUBY-ACTIONPACK-5741907**](https://security.snyk.io/vuln/SNYK-RUBY-ACTIONPACK-5741907)

[**https://www.cve.org/CVERecord?id=CVE-2023-28362**](https://www.cve.org/CVERecord?id=CVE-2023-28362)

[**https://discuss.rubyonrails.org/t/cve-2022-22577-possible-xss-vulnerability-in-action-pack/80533**](https://discuss.rubyonrails.org/t/cve-2022-22577-possible-xss-vulnerability-in-action-pack/80533)

**Contact Details**

Gaurish Bhatia

S222187151@deakin.edu.au

**Pentest Leader Feedback.**

The vulnerability has already been found