

**Finding Name:** Web cache poisoning

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

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

**Finding Description**

Web cache poisoning is a method to exploit the vulnerability, which helps the attacker to store malicious content in the web server. This data then gets transferred to the users machine on visiting the website. The attackers basically exploit the weakness of the storage method of info in caches, which allows them to inject their own content to the cache and could deliver fake information to the users.

**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 web cache poisoning could result in the loss of revenue to the business as if the users are redirected to malicious websites, they will lose trust in the website and will no longer continue to use it which will ultimately lead to loss in revenue to the business. As the users lose confidence, this will lead to damage in the reputation of the company. Furthermore, the IT teams will have to purge the caches in order to fix the issue which will lead to waste in resources.

**Affected Assets**

The affected assets include the Ontrack server, which might have malicious data injected by the attacker leading to spread of the malware on the users systems. Further, the website data may be stolen by the attacker.

**Evidence**

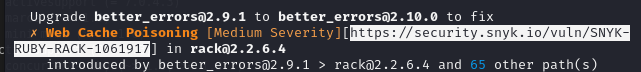
**A screenshot of a computer

Description automatically generated**The following screenshot shows the line of the vulnerable code :

**The affected file path: doubtfire-deploy/gemfile.lock**

As it could be seen on line 250, the better errors version is 2.9.1, which is vulnerable to web cache poisoning.

Further, the following screenshots show that the rack package’s better errors is vulnerable to web cache poisoning:



A screenshot of a computer

Description automatically generated

Further, the following screenshots show more detail 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 rack package to versions newer than 3.0.0.beta 1 would mitigate this vulnerability in full.

**References**

[**https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917**](https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917)

[**https://cwe.mitre.org/data/definitions/444.html**](https://cwe.mitre.org/data/definitions/444.html)

[**https://portswigger.net/web-security/web-cache-poisoning**](https://portswigger.net/web-security/web-cache-poisoning)

**Contact Details**

Gaurish Bhatia

S222187151@deakin.edu.au

**Pentest Leader Feedback.**

The vulnerability has already been found