

**Finding Name: Open Redirect.**

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

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

**Finding Description**

An open redirect vulnerability is a sort of security problem that occurs when a web application sends visitors to a specific URL without sufficient validation. Attackers can use this vulnerability to reroute visitors to malicious websites, phishing pages, and other dangerous material.

**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**

**Affected Assets**

doubtfire-web\src\app\sessions\states\sign-in\sign-in.component.ts

**Evidence**

**Step 1.**

****

**Remediation Advice**

Encode provided URLs to prevent injection of malicious code.

try {

chrome.extension.getBackgroundPage().tgs.setViewGlobals(global, 'options');

} catch (e) {

window.setTimeout(() => window.location.reload(), 1000);

**References**

Snyk CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

OWASP Cheat Sheet Series, <https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html>

**Contact Details**

Shamail Haider

S222408241@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.