

**Finding Name: Unchecked Integrity of resource**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Pushkar Goel | SCR | SCR Team Member | Ontrack | Natalia Khbotova | Yes |
| Jaspriya Kaur | SCR | SCR Team Lead | Ontrack | Natalia Khbotova | Yes |

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

**Finding Description**

Remote artifact is being used in the script tag without checking its integrity which can lead to the unexpected execution of malicious code in the application.

This happens in the following code in **doubtfire-web/src/index.html** where the link is added to script tag without any checks



**Path : doubtfire-web/src/index.html**

On the client side, where front-end code is executed, malicious code could:

* impersonate users' identities and take advantage of their privileges on the application.
* add quiet malware that monitors users' session and capture sensitive secrets.
* gain access to sensitive clients' personal data.
* deface, or otherwise affect the general availability of the application.

Putting an integrity check would allow that the artifact is as expected and is not modified by any malware.

**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**

The modified script which arises due to the insecure code can have severe business implications. It allows attackers to inject malicious scripts into web applications, compromising the security and integrity of the system. The impact includes theft of sensitive data such as student data such as grades, personal details, and academic records as well as login credentials. Moreover, This can disrupt the OnTrack operations by defacing websites, redirecting users to malicious sites, or spreading malware. Also, the stolen information can be used by attackers to conduct spear phising campaign using the leaked information

**Affected Assets**

* Data assets
* Web Application
* Server Infrastructure
* Regulatory Compliance

**Remediation Advice**

* Create a hash of the expected artifact with algorithm like SHA512, SHA384 or SHA256. Then when its being used, we can verify the integrity of resource by cross verifying it with the expected hash

script async src="<https://www.googletagmanager.com/gtag/js?id=G-VJWZRWYE2C>"  
integrity= “sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC”>

**Contact Details**

Pushkar Goel – s222162584@deakin.edu.au

**Secure Code Review Leader Feedback.**