

**Finding Name: Use of password hash with insufficient computational effort.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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**

Using password hashes with insufficient computing effort, such as MD5, offers a serious security concern since they are vulnerable to a variety of attacks, including brute force and rainbow tables. MD5 is recognised to be unsafe, hence it should not be used to hash passwords in current systems. It is critical to shift to more secure hashing algorithms in order to adequately protect user credentials.

**Risk Rating**  
Impact: Minor  
Likelihood: Unlikely

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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**

Using weak algorithm allows attackers to, manipulate data integrity, and impersonate genuine businesses. Unauthorised access to sensitive information, reputational harm, and legal obligations are all potential outcomes of such security breaches. SHA-1 is being deprecated and phased out in favour of more secure hashing algorithms such as SHA-256, therefore utilising it may cause compatibility difficulties with newer cryptographic protocols, software libraries, and security solutions.

**Affected Assets**

doubtfire-web\src\app\common\user-icon\user-icon.component.ts.

Line 39.

**Evidence**

**Step 1.**

**A computer screen shot of a program code

Description automatically generated**

**Remediation Advice**

MD5 hash (used in ts-md5/dist/md5.Md5.hashStr) is insecure. Consider changing it to a secure hashing algorithm.

return crypto.createHash('sha256')

SHA-256 provides longer hash values 256 bits, it is more resistant to collision attacks, where two different inputs produce same hash output.

**References**

CWE-916: Use of Password Hash With Insufficient Computational Effort

[**https://cwe.mitre.org/data/definitions/916.html**](https://cwe.mitre.org/data/definitions/916.html)

Use of Password Hash With Insufficient Computational Effort, Martello Security.

[**https://www.martellosecurity.com/kb/mitre/cwe/916/**](https://www.martellosecurity.com/kb/mitre/cwe/916/)

**Contact Details**

Shamail Haider

S222408241@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.