

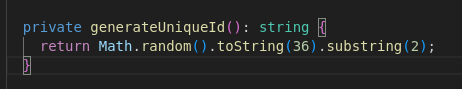
**Finding Name: Weak pseudorandom number generators for User ID**

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

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

**Finding Description**

A weak pseudorandom number generator is being used to generate a userUniqueID through the function **generateUniqueId()** in the file **doubtfire-web/src/app/common/user-icon/user-icon.component.ts**



When software generates predictable values in a context requiring unpredictability, it may be possible for an attacker to guess the next value that will be generated, and use this guess to impersonate another user or access sensitive information.

Using pseudorandom number generators (PRNGs) is security-sensitive. For example, it has led in the past to the following vulnerabilities:

* CVE-2013-6386
* CVE-2006-3419
* CVE-2008-4102

**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**

Security vulnerabilities in PRNGs (pseudorandom number generators ) can lead to unauthorized access to student data, compromising confidentiality and privacy. This could result in data breaches, exposing sensitive information such as grades, personal details, and academic records. Moreover, security incidents could disrupt the submission process, causing delays and inconvenience for students and instructors. Also, the stolen information can be used by attackers to conduct spear phising campaign using the leaked information

**Affected Assets**

This vulnerability will affect the student data, as its confidentiality will be compromised if an attack is successful. This will also impact system infrastructure as this can allow lateral movement within the platform disrupting the functioning of OnTrack's portal infrastructure, causing downtime, delays in assignment submissions, and inconvenience for users

**Remediation Advice**

* Use a cryptographically strong pseudorandom number generator (CSPRNG) like crypto.getRandomValues().
* Use the generated random values only once.
* Do not expose the generated random value. If it has to be stored, it should be made sure that the database or file is secure.

**References**

* MITRE CVE

**Contact Details**

Pushkar Goel – s222162584@deakin.edu.au

**Secure Code Review Leader Feedback.**

The lead will provide feedback to enact on.