

**Finding Name:** Potential Path traversal

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Gaurish Bhatia | SCR | SCR team member | Ontrack | Payas Paul and Jaspriya Kaur |  |

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

**Finding Description**

The path traversal or directory traversal vulnerability is a flaw, which could lead to potential attacks when the application uses direct file path in the application, which could be manipulated by the user, which could lead to unauthorized access to the directories or files located, which are having sensitive information.

**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**

Using direct path to retrieve a file without sanitization of the path, could potentially lead an attacker to get access to the file structure by the means of which the files are stored in the server, it could also lead to unauthorized access to the files by the attacker, this could lead to disclosure of sensitive information.

**Affected Assets**

doubtfire-deploy\doubtfire-api\api\submission\portfolio\_evidence\_api.rb

line: 113

**Evidence**

The following screenshot shows the line of the vulnerable code:

A screen shot of a computer program

Description automatically generated

As it could be seen on line 113, in which the File.read function directly uses the evidence\_loc, which is the location of the file for the portfolio submission as per the given case, it could be seen that the evidence\_loc directly stores the file path through line 90, which could be a potential threat leading to a path traversal attack. Further, if the evidence\_loc is nil, it could open the file directory structure to the user as it uses the line Rails.root.join('public', 'resources', 'FileNotFound.pdf').

**Remediation Advice**

Specifically, the following remedial methodologies could be used to mitigate this vulnerability:

* A base directory could be defined, where files could be stored and could be accessed. For an instance, all the files that are to be accessed could be listed on a single directory and the path to access the files could be restricted to the particular directory only. Example: base\_directory = Rails.root.join(‘public’, ‘resources’).
* The input parameters should be validated before retrieving the path via the input, which would ensure that the files are not prone to any of the injection attacks.
* The proper sanitization of the paths should be done to ensure that the potential attacker could not navigate outside of the base directory, also, the use of ‘File.join’ should be used in order to link the base directory with the file name. this could be done in the form of the following commands:

1. filename = task.processing\_pdf? ? 'AwaitingProcessing.pdf' : "# {task.task\_definition.abbreviation}.pdf"
2. evidence\_loc = File.join(base\_dir, filename)

**References**

[**https://portswigger.net/kb/issues/00100300\_file-path-traversal**](https://portswigger.net/kb/issues/00100300_file-path-traversal)

[**https://owasp.org/www-community/attacks/Path\_Traversal**](https://owasp.org/www-community/attacks/Path_Traversal)

**Contact Details**

Gaurish Bhatia

S2221987151@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.