

**Finding Name: PATH TRAVERSAL**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Payas Paul | SCR | Senior Lead | Ontrack | Jaspriya kaur |  |
|  |  |  |  |  |  |

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

# **Finding Description**

The `TaskDownloadsController` in the Ontrack project lacks proper sanitization measures for user-generated input used in generating the `download\_id` at line 48. This oversight exposes the application to potential path manipulation vulnerabilities, allowing attackers to manipulate filenames and potentially perform directory traversal attacks. This could lead to unauthorized access to sensitive files or compromise the integrity of the file download process. Urgent remediation is advised to implement robust input validation and sanitization to mitigate this risk effectively.

**Risk Rating**

Impact: **Significant**Likelihood: **High**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 vulnerability's exploitation could lead to various negative consequences for the company and the application:

1. **Data Leakage:** Sensitive data transmitted during file downloads could be intercepted, leading to data leakage and potential compliance violations.
2. **Reputation Damage:** Public disclosure of sensitive information could harm the company's reputation and erode customer trust.
3. **Legal Consequences:** Non-compliance with data protection regulations could result in legal penalties and financial losses.

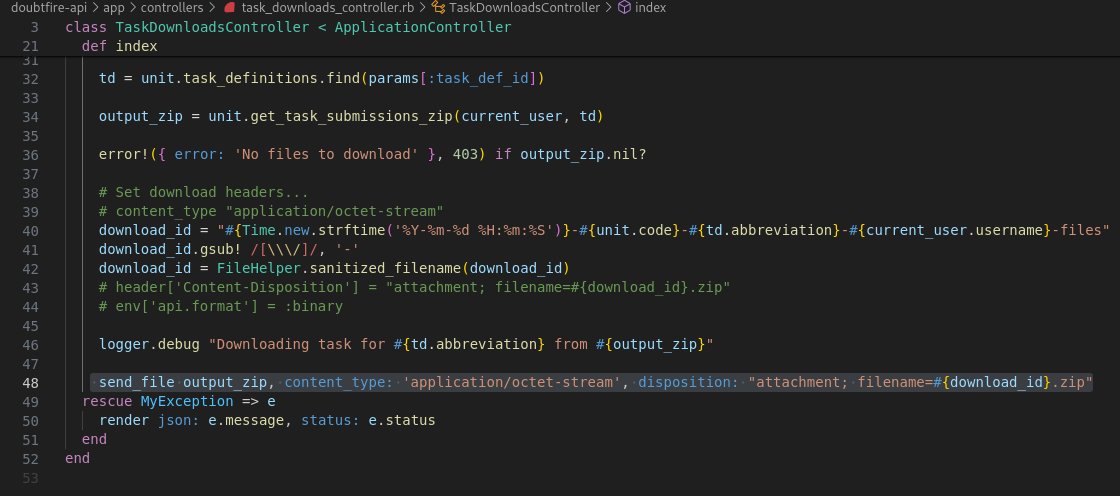
# **Affected Assets**

The primary affected asset in this vulnerability is the TaskDownloadsController within the Ontrack(The following URLs are impacted: localhost: 4200 (main application) of the project. This controller is responsible for handling requests related to the download of task-related files within the application. Given its central role in facilitating file downloads, any vulnerabilities present in this controller directly impact the security of data exchanged during this process.

# **Evidence**

**STEP 1:**

Path: /doubtfire-deploy/doubtfire-api/controllers/task\_downloads\_controller.rb, line 48.



Step 2: Run the main application to access the TaskDownloadsController.

Step 3: Identify the absence of proper sanitization measures in the TaskDownloadsController for user-generated input used in generating the download\_id at line 48.

Step 4: Understand the potential risks associated with the vulnerability:

# **Remediation Advice**

To mitigate this vulnerability, it's recommended to implement encryption for communications during file downloads. This can be achieved by:

* Utilizing HTTPS (TLS/SSL) for secure communication between the server and clients.
* Ensuring that file downloads are encrypted using appropriate cryptographic protocols and algorithms.

# **References**

[**https://www.synopsys.com/glossary/what-is-path-traversal.html#:~:text=A%20path%20traversal%20vulnerability%20allows,of%20the%20web%20root%20folder**](https://www.synopsys.com/glossary/what-is-path-traversal.html#:~:text=A%20path%20traversal%20vulnerability%20allows,of%20the%20web%20root%20folder)**.**

**Snyk tool**

# **Contact Details**

Payas Paul

612payaspaul@gmail.com

**Pen test Leader Feedback.**

The lead will provide feedback to enact on.