

**Finding Name:** Path Transversal.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Payas Paul | SCR | Senior Lead | Ontrack | Roocha T, Charanpree |  |
|  |  |  |  |  |  |

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

**Finding Description**

Path Traversal, also known as Directory Traversal,

A vulnerability that allows an attacker to access files and directories that are outside the intended directory.

**Risk Rating**  
Impact: Major  
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**

**Impact on the Company**

Data Breach: If attackers are able to access sensitive data, there could be a data breach that has negative effects on reputation, law, and regulation.

System Compromise: If an attack is successful, the attackers may be able to take over the server and carry out more malicious actions.

Compliance Issues: If a data breach occurs, the organization may be subject to fines and penalties for violating PCI DSS or GDPR requirements.

**Effect on the Application**

Decreased Trustworthiness: The vulnerability may cause users to lose faith in the security and dependability of the program.

Cost Increases: Time and resources will be needed to resolve the problem, which will raise the cost of development and upkeep.

Possibility of Additional Vulnerabilities: The vulnerability can point to more serious security issues with the creation and design of the application.

**Affected Assets**

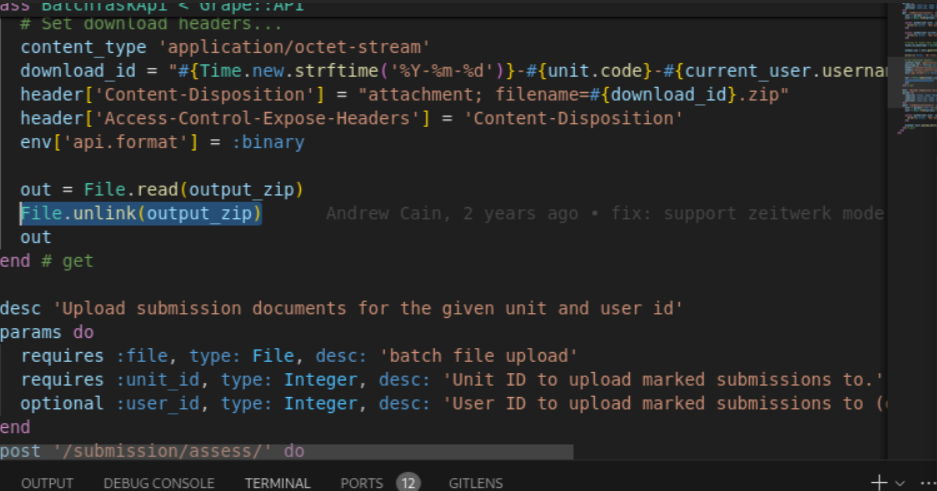
**Sensitive Files and Data**: The server's sensitive files and data may be accessible due to the vulnerability.   
**Server Infrastructure**: A successful vulnerability could give the attacker control of the system and result in a compromise.   
**Application Trustworthiness**: The flaw may cause users to lose faith in the security of the application.   
**Regulation and Compliance Requirements**: Failure to comply with regulations in the event of a data breach may incur fines and penalties.   
**Application Development and Maintenance**: Taking care of the problem will cost more money because it will take time and resources.

**Evidence**

**Step 1.**

In this case, the vulnerability is in the **batch\_task\_api.rb** file on line 45, where unsanitized input is used as a path in the **File.unlink** method.

**Step 2.**

****

**Step 3.**

**Remediation Advice**

**Top mitigate this you should make sure that any user input is thoroughly cleaned and verified before being utilized to create file paths in order to reduce the impact of this vulnerability. A whitelist of permitted characters or a library or method that securely creates file paths, such File.join() or File.expand\_path(), can be used to accomplish this.**

**References**

[**https://github.com/botesjuan/Burp-Suite-Certified-Practitioner-Exam-Study**](https://github.com/botesjuan/Burp-Suite-Certified-Practitioner-Exam-Study)

**OWASP WebGoat** - <https://owasp.org/www-community/attacks/Path_Traversal>

**Snyk**

**Portswigger web security academy**

**Contact Details**

Payas Paul (Senor Lead)

[612payaspaul@gmail.com](mailto:612payaspaul@gmail.com)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.