

**Finding Name:** Insecure File Type Handling

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Deakin Carr | SCR | Junior Team Member | Ontrack |  |  |
|  |  |  |  |  |  |

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

**Finding Description**

The Ontrack application exhibits a significant security vulnerability in its file upload mechanism. Specifically, the DiscussionCommentApi class allows users to attach files to discussion comments without adequate validation of the file type or content. While the application checks for the presence of an attachment and verifies that its size is less than 30MB, it neglects to assess the nature of the file, opening the door for the upload of potentially harmful content.

**Risk Rating**  
Impact: **Major**  
 This vulnerability holds a major impact because, if exploited, it could allow the upload of malicious files, leading to unauthorized access or malware distribution. This would significantly impede regular activities of the Ontrack application, affecting the educational process and potentially leading to the compromise of sensitive data.  
  
Likelihood: **Moderate**  
 Given the specifics of the vulnerability and the potential for exploitation by individuals with some technical know-how, the likelihood is moderate. The vulnerability may be exploited if discovered by attackers, especially in a university setting where individuals often have the necessary technical skills.

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

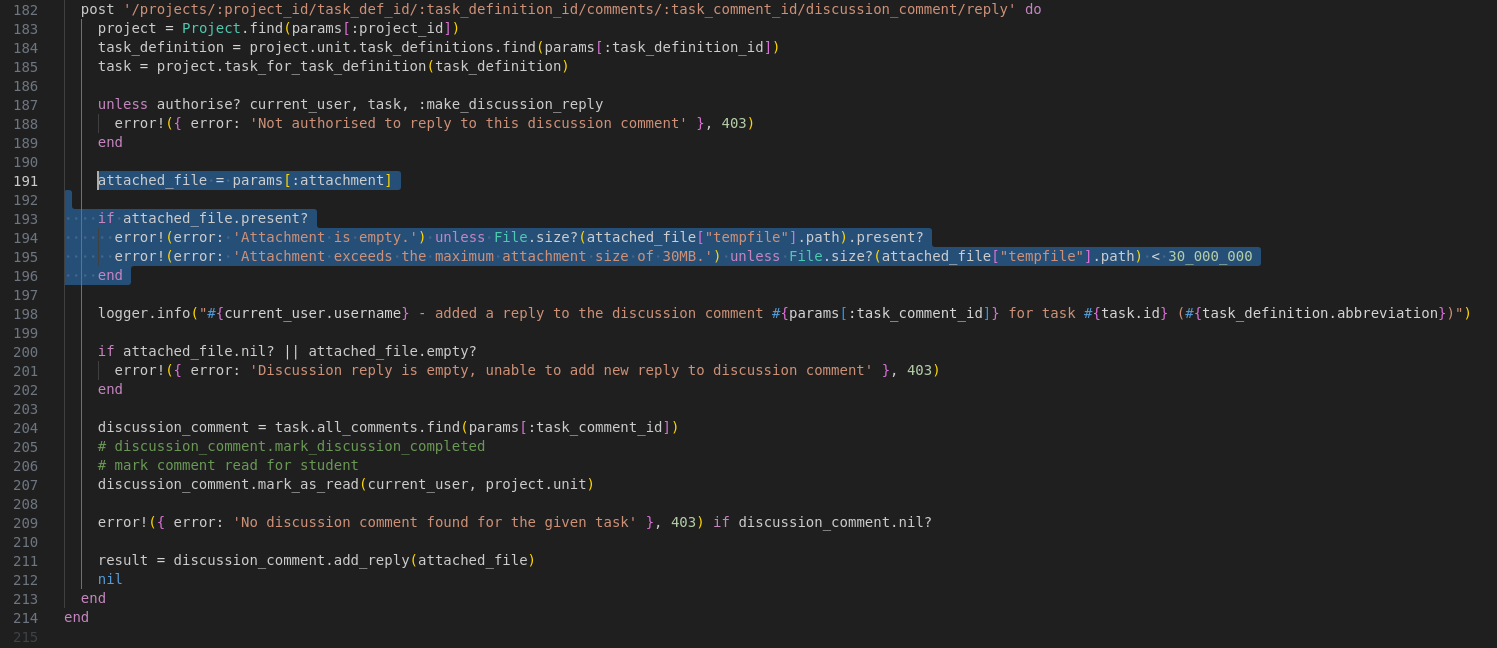
The identified vulnerability poses a serious threat to the integrity and security of the Ontrack application and its users. Malicious actors could exploit this loophole to upload executable scripts or files containing harmful content, leading to unauthorized access, data leakage, or the spread of malware within the university's network. Such breaches could disrupt the educational process, damage the institution's reputation, and result in substantial financial losses due to potential legal action and remediation efforts.

**Affected Assets**

The primary asset affected by this vulnerability is the Ontrack application's server and its stored data, including sensitive student and faculty information. The angular js front end, while not directly impacted by the file upload vulnerability, could allow students and teachers to easily access malicious files uploaded via the unsafe upload mechanism.

**Evidence**

The vulnerability was identified within the post '/projects/:project\_id/task\_def\_id/:task\_definition\_id/discussion\_comments' endpoint in the DiscussionCommentApi class located in /doubtfire-api/app/api/discussion\_comment\_api.rb. The code segment responsible for handling file attachments lacks proper validation mechanisms to ensure the safety and appropriateness of the uploaded files. This oversight was observed in the handling of params[:attachments], where the application only checks for file presence and size constraints.



**Remediation Advice**

To mitigate this vulnerability, the following measures are recommended:

* Implement comprehensive file validation: The application should validate the MIME type and content of the uploaded files to ensure they are safe and meet the intended use criteria.
* Employ file scanning: Integrate antivirus or malware scanning tools to examine files at the point of upload, preventing the storage or distribution of malicious content.
* Enforce strict access controls: Ensure that file upload and retrieval functionalities are accessible only to authenticated and authorized users, minimizing the potential for unauthorized actions.
* Conduct regular security audits: Regularly review and test the application's security measures to identify and address new vulnerabilities promptly.

Addressing this vulnerability is crucial for maintaining the security and reliability of the Ontrack application, safeguarding the university's digital assets, and ensuring a safe environment for its users.

**References**

ChatGPT, “ChatGPT”, OpenAI [Large language model] Available: [https://chat.openai.com](https://chat.openai.com/) [Accessed: 2/4/2024].

**Contact Details**

Deakin Carr

Carrde@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.