Review a file-upload advisory

Work with a partner to review a real advisory and a small GitHub application. Recommend what the team should do and support your decision with evidence.

Scenario

Assume our team runs the linked code and locked dependencies as a public service for customer support attachments. Anyone can reach the upload endpoint. Support staff need the files to resolve requests, but customers can email attachments while uploads are disabled. There is no evidence of an attack yet. These deployment and workflow details are scenario assumptions.

A teammate says:

> “We already limit each request to 12 files and handle upload errors, so we can leave uploads running until next week.”

Open these sources

Start here: github.com/cmu-devops/activity-nodejs-simple-file-upload

To find the advisory, search for GHSA-v52c-386h-88mc.

Read the advisory and inspect the repository. Find the installed Multer version and where the app handles uploads.

Multer is a Node.js package for handling file uploads.

Your task

Answer the three questions on page 2. Use what you find in the advisory and code to explain your reasoning.

Your review

Names: _____

1. Do you agree with your teammate?

Do the file limit and error handling address the problem described in the advisory? Use the advisory and code to explain your answer.

2. What should the team do today?

Keep uploads available or use email while fixing the problem? Explain your choice and what needs to change.

3. How would you check the repair?

What would you test before restoring uploads? How would you check that the updated package is running?