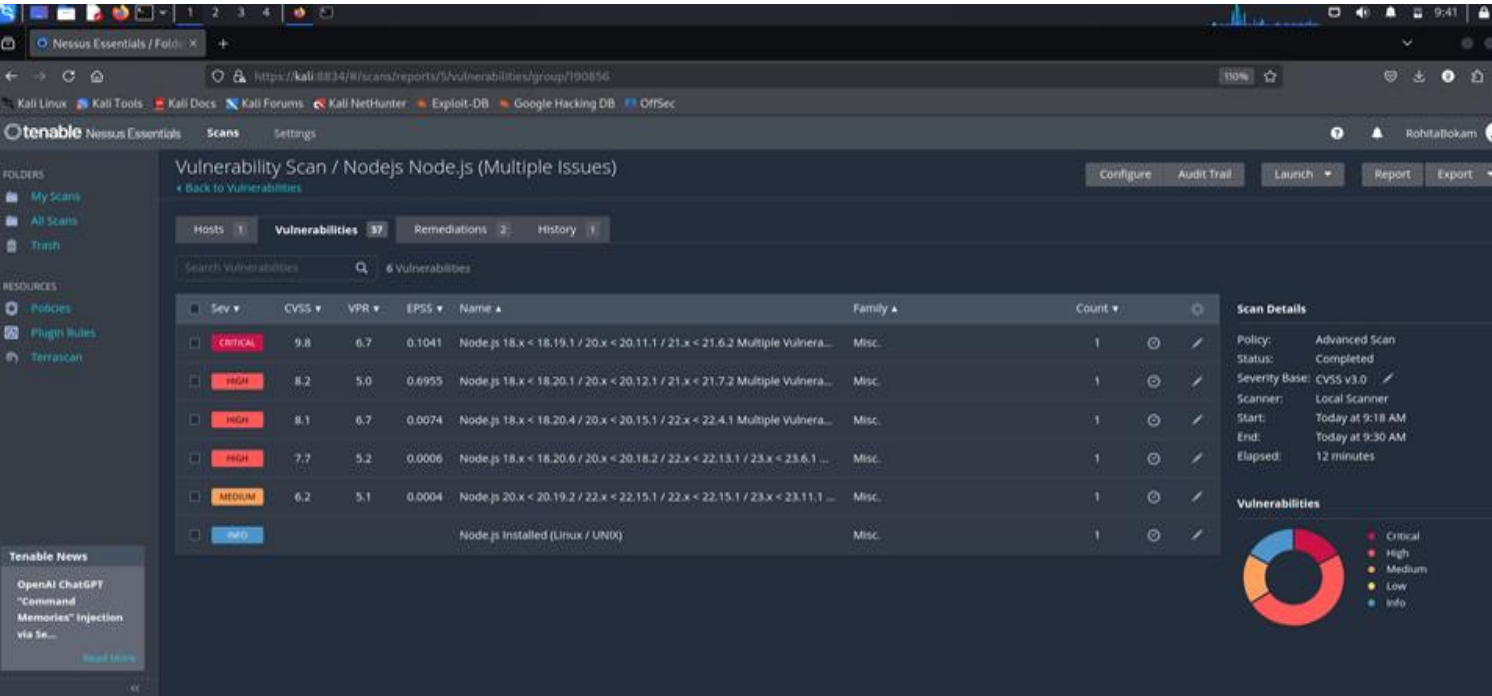


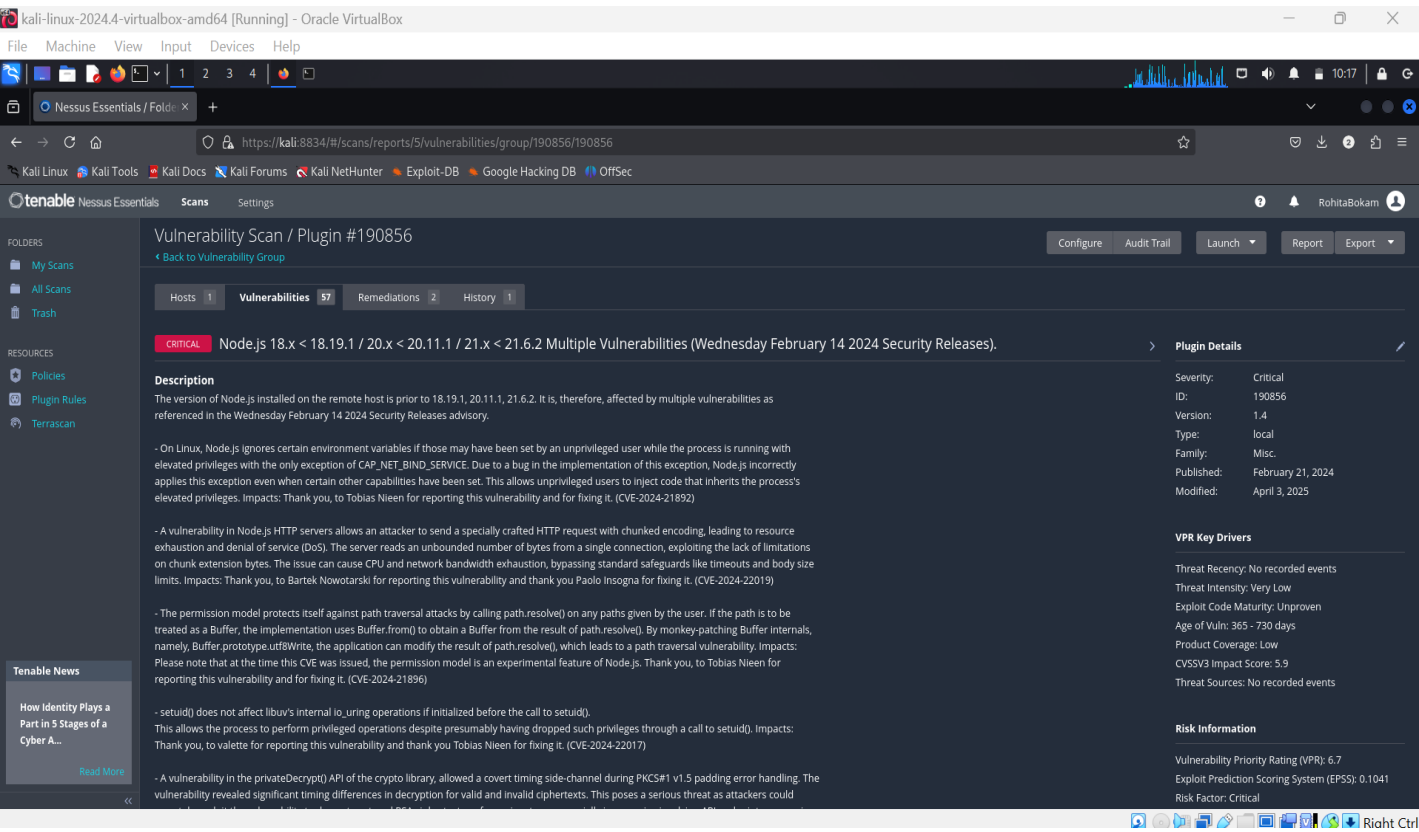
# Documentation of most critical vulnerability in my PC:

## IP address :10.0.2.15

## Here's the most critical vulnerability in my PC



## And here's the description and solution the critical vulnerability:



The screenshot displays the Nessus Essentials web interface. The top navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main header shows the Tenable logo and navigation tabs for Nessus Essentials, Scans, and Settings.

The left sidebar contains sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Terrascan). A "Tenable News" section at the bottom left highlights "Cloud Data Protection: How DSPM Helps You Discover..." with a "Read More" link.

The main content area displays a vulnerability report for Node.js. It includes a detailed description of the issue, its impacts, and a solution. Below the solution, there is a "See Also" section with a link to a Nessus update page. The "Output" section shows the path, installed version, and fixed version of the affected package. At the bottom, a table lists the port and host details for the scan.

**Vulnerability Description:**

implementations leading to filesystem permission model bypass through path traversal attack. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to xion for reporting this vulnerability and thank you Rafael Gonzalez for fixing it. (CVE-2024-21891)

- The Node.js Permission Model does not clarify in the documentation that wildcards should be only used as the last character of a file path. For example: --allow-fs-read=/home/node/.ssh/\*.pub will ignore pub and give access to everything after .ssh/. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Niesen for reporting this vulnerability and thank you Rafael Gonzalez for fixing it. (CVE-2024-21890)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

**Solution**

Upgrade to Node.js version 18.19.1 / 20.11.1 / 21.6.2 or later.

**See Also**

<http://www.nessus.org/u?313add11>

**Output**

```
Path          : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version  : 20.11.1
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	10.0.2.15

# -Rohita B