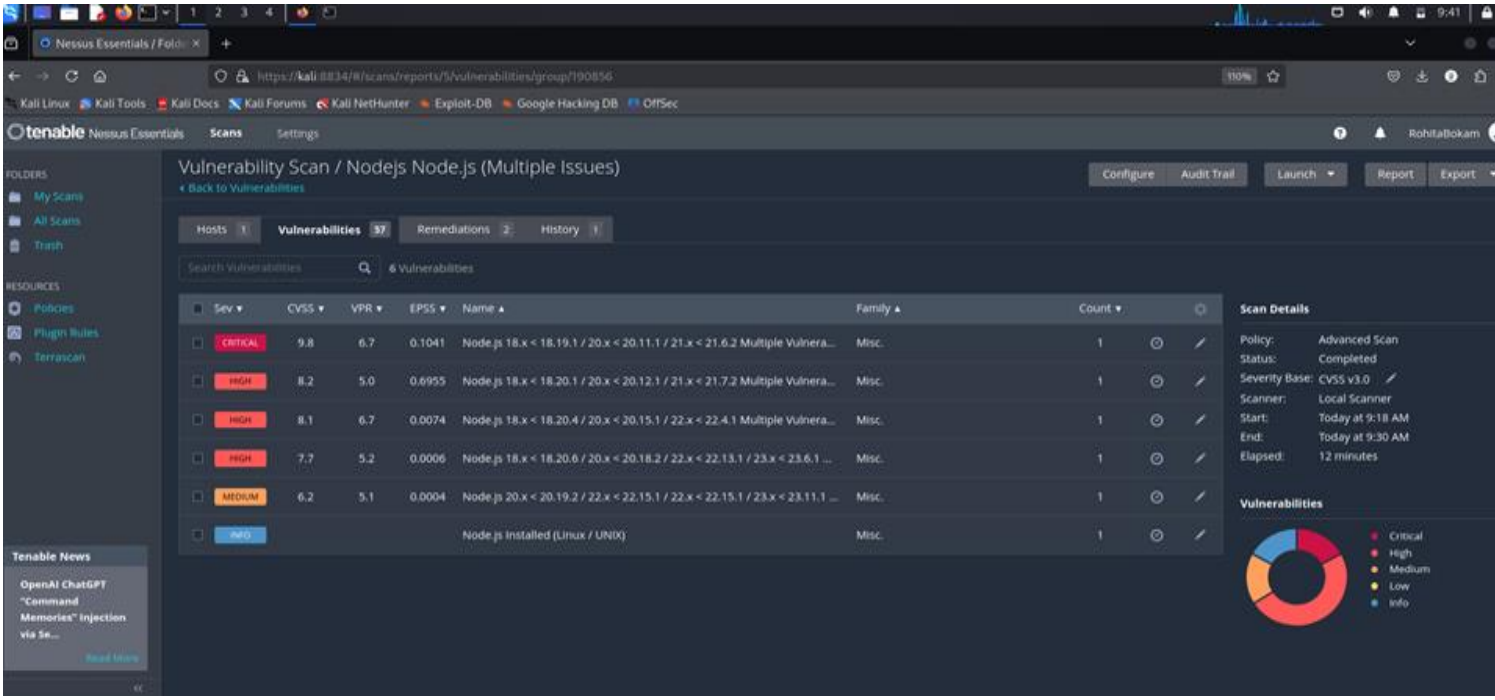
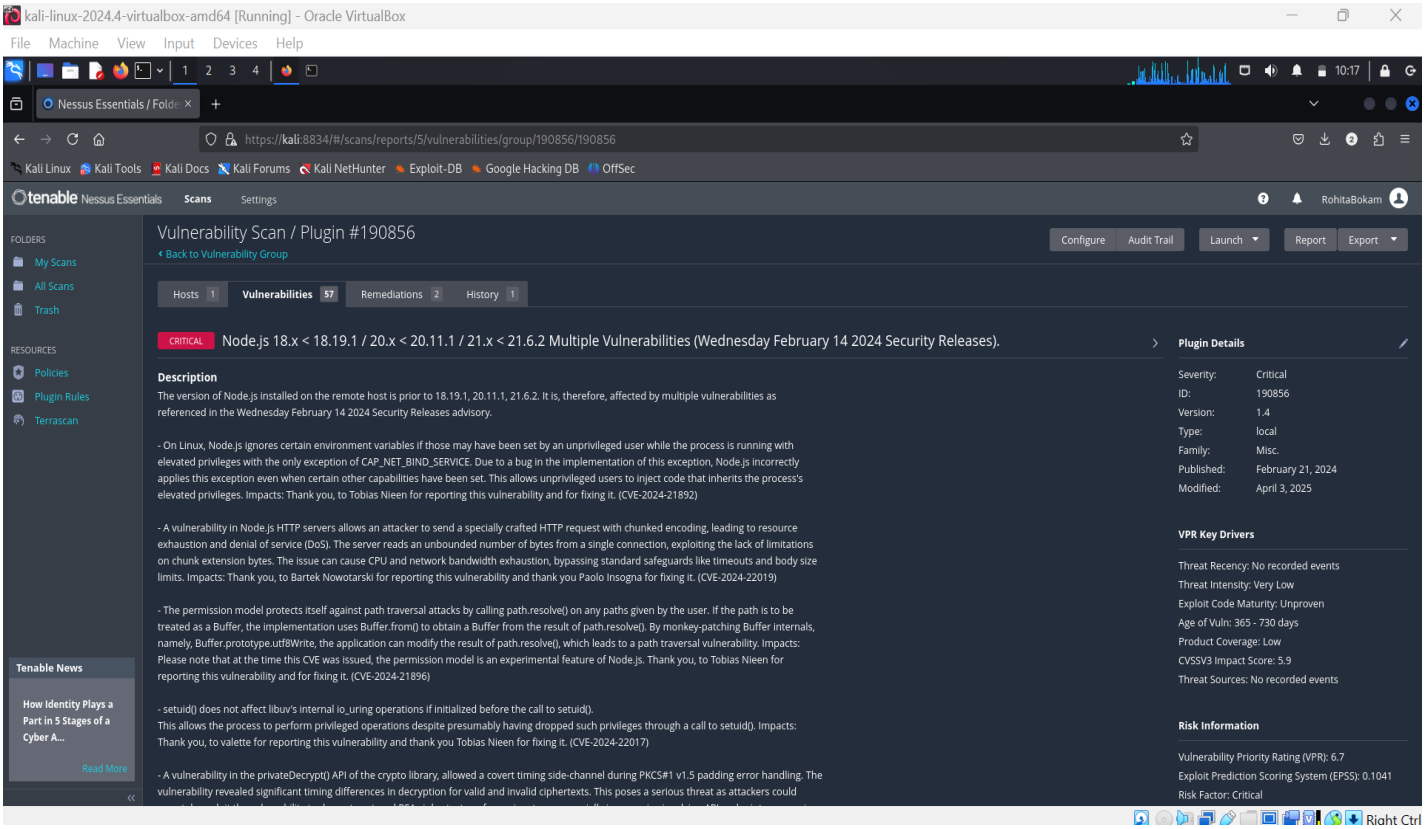
Documentation of most critical vulnerability in my PC:

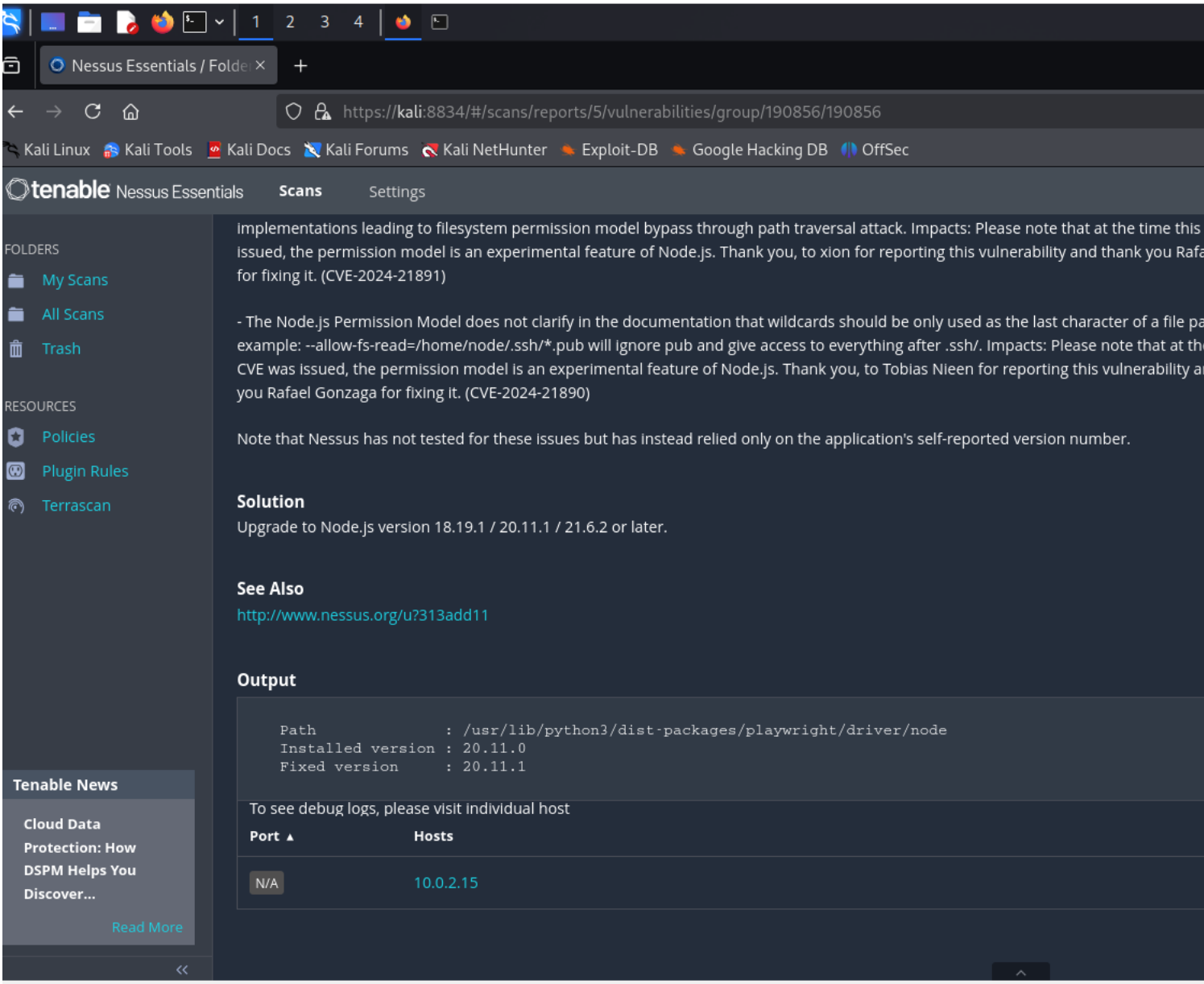
IP address :10.0.2.15

Here’s the most critical vulnerability in my PC



And here’s the description and solution the critical vulnerability:




1 2 3 4
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/5/vulnerabilities/group/190856/190856
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cloud Data Protection: How DSPM Helps You Discover...
Read More
implementations leading to filesystem permission model bypass through path traversal attack. Impacts: Please note that at the time this
issued, the permission model is an experimental feature of Node.js. Thank you, to xion for reporting this vulnerability and thank you Rafa
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 pa
example: --allow-fs-read=/home/node/.ssh/*.pub will ignore pub and give access to everything after .ssh/. Impacts: Please note that at th
CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Nieen for reporting this vulnerability a
you Rafael Gonzaga 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