Nessus și scorul CVSS oferă organizațiilor instrumente puternice pentru a evalua, monitoriza și gestiona vulnerabilitățile din infrastructura lor IT. Scorul CVSS (Common Vulnerability Scoring System) furnizat de scanere (Nessus) ajută la evaluarea și prioritizarea vulnerabilităților identificate.

https://www.cvedetails.com/

CVSS (Common Vulnerability Scoring System) este un sistem standardizat pentru evaluarea și atribuirea scorurilor vulnerabilităților în domeniul securității informatice. Scopul acestui sistem este de a oferi o metodă obiectivă și uniformă pentru măsurarea gravității vulnerabilitătilor în sistemele informatice.

CVSS oferă un set de metrici care sunt evaluate pentru a genera un scor numeric final, cunoscut sub numele de CVSS Score. Acest scor este util pentru a ajuta organizațiile să prioritizeze și să gestioneze eficient vulnerabilitățile în infrastructura lor IT.

Principalele componente ale CVSS includ:

Base Score - evaluează caracteristicile fundamentale ale unei vulnerabilități și este alcătuită din trei grupuri de metrici:

- 1. **Exploitability Metrics:** Evaluază cât de ușor poate fi exploatată vulnerabilitatea.
- 2. **Impact Metrics:** Măsoară gravitatea impactului asupra sistemului în cazul unei exploatări.
- 3. **Scope Metrics:** Determină dacă vulnerabilitatea afectează sau nu alte componente ale sistemului.

Temporal Score - reflectă schimbările în timp legate de expunere și remedierea vulnerabilității.

Environmental Score - reflectă caracteristicile specifice ale mediului în care sistemul este implementat.

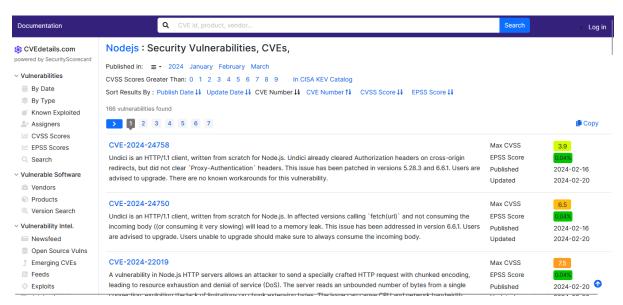
Scorul CVSS poate varia de la 0.0 (cel mai puţin grav) la 10.0 (cel mai grav). Cu cât scorul este mai mare, cu atât vulnerabilitatea este considerată mai gravă.

CVSS furnizează informații detaliate pentru a ajuta analiștii de securitate să înțeleagă riscul și impactul unei vulnerabilități și să decidă asupra priorității de remediere. Este important să se înțeleagă că scorul CVSS reprezintă o măsură obiectivă a gravității unei vulnerabilități și nu poate acoperi toate aspectele unice ale unui mediu specific. De aceea, trebuie utilizat împreună cu o analiză cuprinzătoare a contextului specific al fiecărei organizații.

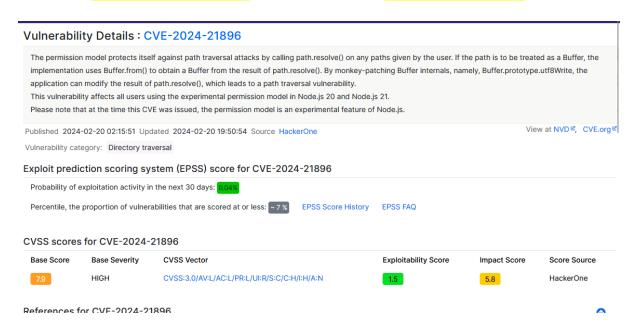
Studiu practic. Sa se analizeze in detaliu minim 3 vulnerabilitati specifice tehnologiilor folosite in realizarea aplicatiilor practice de la lucrarea de licenta.

Exemplu:

Daca in lucrarea de licenta folositi tehnologia node.js atunci:faceti o cautare cu privire la node js cve details



Alegeti minim 3 vulnerabilitati cu scor >7 si analizatile folosind inclusiv descrierea acestora in https://nvd.nist.gov/vuln, exemplu de cautare: CVE-2024-21896 nist



斯CVE-2024-21896 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

The permission model protects itself against path traversal attacks by calling path.resolve() on any paths given by the user. If the path is to be treated as a Buffer, the implementation uses Buffer,from() to obtain a Buffer from the result of path.resolve(). By monkey-patching Buffer internals, namely, Buffer.prototype.utf8Write, the application can modify the result of path.resolve(), which leads to a path traversal vulnerability. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 21. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.

QUICK INFO CVE Dictionary Entry: CVE-2024-21896 NVD Published Date: 02/19/2024 NVD Last Modified: 02/20/2024 Source:

HackerOne



References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://hackerone.com/reports/2218653	

Daca nu v-ati decis asupra tehnologiile folosite in lucrarea de licenta analizati 3 vulnerabiliti cu scorul peste 8 din raportul de scanare furnizat de Nessus care este incarcat in folderul curent.