

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 vulnerabilităților 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 exploatare.
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 puțin 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**

Documentation

CVE id, product, vendor...

Search

Log in

CVEdetails.com

powered by SecurityScorecard

Vulnerabilities

By Date

By Type

Known Exploited

Assigners

CVSS Scores

EPSS Scores

Search

Vulnerable Software

Vendors

Products

Version Search

Vulnerability Intel.

Newsfeed

Open Source Vulns

Emerging CVEs

Feeds

Exploits

Nodejs : Security Vulnerabilities, CVEs,

Published in: 2024 January February March

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

166 vulnerabilities found

1 2 3 4 5 6 7

Copy

CVE-2024-24758

Undici is an HTTP/1.1 client, written from scratch for Node.js. Undici already cleared Authorization headers on cross-origin redirects, but did not clear 'Proxy-Authentication' headers. This issue has been patched in versions 5.28.3 and 6.6.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.

Max CVSS

EPSS Score

Published

Updated

3.9

0.04%

2024-02-16

2024-02-20

CVE-2024-24750

Undici is an HTTP/1.1 client, written from scratch for Node.js. In affected versions calling 'fetch(url)' and not consuming the incoming body (or consuming it very slowly) will lead to a memory leak. This issue has been addressed in version 6.6.1. Users are advised to upgrade. Users unable to upgrade should make sure to always consume the incoming body.

Max CVSS

EPSS Score

Published

Updated

6.5

0.04%

2024-02-16

2024-02-20

CVE-2024-22019

A vulnerability in Node.js HTTP servers allows an attacker to send a specially crafted HTTP request with chunked encoding, leading to resource exhaustion and denial of service (DoS). The server reads an unbounded number of bytes from a single connection, eventually hitting the limit of available memory. This is a regression of a fix in Node.js 16.17.0.

Max CVSS

EPSS Score

Published

Updated

7.5

0.04%

2024-02-20

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**

Vulnerability Details : CVE-2024-21896

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.

Published 2024-02-20 02:15:51 Updated 2024-02-20 19:50:54 Source HackerOne

View at NVD CVE.org

Vulnerability category: Directory traversal

Exploit prediction scoring system (EPSS) score for CVE-2024-21896

Probability of exploitation activity in the next 30 days: 0.04%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 7 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2024-21896

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
7.9	HIGH	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N	1.5	5.8	HackerOne

References for CVE-2024-21896

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

Severity

CVSS Version 3.x

CVSS Version 2.0


CVSS 3.x Severity and Metrics:

 NIST: NVD

Base Score:

N/A

NVD score not yet provided.

 CNA: HackerOne

Base Score:

7.3 HIGH

Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings. A CNA provided score within the CVE List has been displayed.

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.

Hypertlink	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.