



CVE-2021-44531

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-44531 |
| State | PUBLIC |
| Assigner | support@hackerone.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-02-24 19:15:00 UTC |
| Updated | 2022-10-05 13:56:00 UTC |
| Description | Accepting arbitrary Subject Alternative Name (SAN) types, unless a PKI is specifically defined to use a particular SAN type, |

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------------------|---|----------|--------|---------|----------|
| Application | Nodejs | Node.js | All | All | All | All |
| Application | Oracle | Graalvm | 20.3.5 | All | All | All |
| Application | Oracle | Graalvm | 21.3.1 | All | All | All |
| Application | Oracle | Graalvm | 22.0.0.2 | All | All | All |
| Application | Oracle | Mysql Cluster | All | All | All | All |
| Application | Oracle | Mysql Connectors | All | All | All | All |
| Application | Oracle | Mysql Enterprise Monitor | All | All | All | All |
| Application | Oracle | Mysql Server | All | All | All | All |
| Application | Oracle | Mysql Server | All | All | All | All |
| Application | Oracle | Mysql Workbench | All | All | All | All |
| Application | Oracle | Peoplesoft Enterprise Peopletools | 8.58 | All | All | All |
| Application | Oracle | Peoplesoft Enterprise Peopletools | 8.59 | All | All | All |

References

| Reference | Source | Link | Tags |
|---|--------|-------------------------------|------|
| January 10th 2022 Security Releases Node.js | MISC | nodejs.org | |
| HackerOne | MISC | hackerone.com | |

| | | | |
|---|---------|---|---------------------|
| March 2022 Node.js Vulnerabilities in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | |
| Oracle Critical Patch Update Advisory - April 2022 | MISC | www.oracle.com | |
| Debian -- Security Information -- DSA-5170-1 nodejs | DEBIAN | www.debian.org | |
| Oracle Critical Patch Update Advisory - July 2022 | N/A | www.oracle.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 160231 Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2022-7830) |
| 160361 Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2022-9073-1) |
| 179565 Debian Security Update for nodejs (DSA 5170-1) |
| 184126 Debian Security Update for nodejs (CVE-2021-44531) |
| 240414 Red Hat Update for rh-nodejs12-nodejs security (RHSA-2022:4914) |
| 240747 Red Hat Update for rh-nodejs14-nodejs (RHSA-2022:7044) |
| 240851 Red Hat Update for nodejs:14 (RHSA-2022:7830) |
| 241026 Red Hat Update for nodejs:16 security (RHSA-2022:9073) |
| 241341 Red Hat Update for nodejs:14 security (RHSA-2023:1742) |
| 282257 Fedora Security Update for nodejs (FEDORA-2022-78090d2099) |
| 282263 Fedora Security Update for nodejs (FEDORA-2022-0eda327cb4) |
| 296062 Oracle Solaris 11.4 Support Repository Update (SRU) 43.113.3 Missing (CPUJAN2022) |
| 354342 Amazon Linux Security Advisory for nodejs : ALAS2022-2022-214 |
| 354509 Amazon Linux Security Advisory for nodejs : ALAS2022-2022-019 |
| 354537 Amazon Linux Security Advisory for nodejs : ALAS-2022-214 |
| 355273 Amazon Linux Security Advisory for nodejs : ALAS2023-2023-084 |
| 376254 Node.js Improper Handling of URI Subject Alternative Names Vulnerability (JAN 2022) |
| 500441 Alpine Linux Security Update for nodejs |
| 501456 Alpine Linux Security Update for nodejs |
| 501973 Alpine Linux Security Update for nodejs |
| 502124 Alpine Linux Security Update for nodejs-current |

| |
|---|
| 502138 Alpine Linux Security Update for openjdk11 |
| 504210 Alpine Linux Security Update for nodejs |
| 690825 Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (972ba0e8-8b8a-11ec-b369-6c3be5272acd) |
| 751613 OpenSUSE Security Update for nodejs12 (openSUSE-SU-2022:0113-1) |
| 751614 OpenSUSE Security Update for nodejs14 (openSUSE-SU-2022:0112-1) |
| 753115 SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2022:0113-1) |
| 753438 SUSE Enterprise Linux Security Update for nodejs14 (SUSE-SU-2022:0112-1) |
| 900726 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (8837) |
| 901262 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (8840-1) |
| 940775 AlmaLinux Security Update for nodejs:14 (ALSA-2022:7830) |
| 940859 AlmaLinux Security Update for nodejs:16 (ALSA-2022:9073) |
| 960636 Rocky Linux Security Update for nodejs:14 (RLSA-2022:7830) |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)