



CVE-2020-8277

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-8277 |
| State | PUBLIC |
| Assigner | support@hackerone.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-11-19 01:15:00 UTC |
| Updated | 2023-11-07 03:26:00 UTC |
| Description | A Node.js application that allows an attacker to trigger a DNS request for a host of their choice could trigger a Denial of Ser |

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------------|--|---------|--------|---------|----------|
| Application | C-ares Project | C-ares | All | All | All | All |
| Application | C-ares Project | C-ares | All | All | All | All |
| Operating System | Fedora project | Fedora | 32 | All | All | All |
| Operating System | Fedora project | Fedora | 33 | All | All | All |
| Operating System | Fedora project | Fedora | 32 | All | All | All |
| Operating System | Fedora project | Fedora | 33 | All | All | All |
| Application | Node.js | Node.js | All | All | All | All |
| Application | Node.js | Node.js | All | All | All | All |
| Application | Node.js | Node.js | All | All | All | All |
| Application | Node.js | Node.js | All | All | All | All |
| Application | Oracle | Blockchain Platform | All | All | All | All |
| Application | Oracle | Gaalvm | 19.3.4 | All | All | All |
| Application | Oracle | Gaalvm | 20.3.0 | All | All | All |
| Application | Oracle | Gaalvm | 19.3.4 | All | All | All |
| Application | Oracle | Gaalvm | 20.3.0 | All | All | All |
| Application | Oracle | Jd Edwards Enterpriseone Tools | All | All | All | All |
| Application | Oracle | Mysql Cluster | All | All | All | All |

| | | | | | | |
|-------------|------------------------|--|--------|-----|-----|-----|
| Application | Oracle | Retail Xstore Point Of Service | 16.0.6 | All | All | All |
| Application | Oracle | Retail Xstore Point Of Service | 17.0.4 | All | All | All |
| Application | Oracle | Retail Xstore Point Of Service | 18.0.3 | All | All | All |
| Application | Oracle | Retail Xstore Point Of Service | 19.0.2 | All | All | All |

References

| Reference | Source | Link |
|---|---------|---|
| [SECURITY] Fedora 33 Update: mingw-c-ares-1.17.1-1.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| [SECURITY] Fedora 33 Update: c-ares-1.17.0-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] Fedora 33 Update: mingw-c-ares-1.17.1-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| Oracle Critical Patch Update Advisory - April 2022 | MISC | www.oracle.com |
| Oracle Critical Patch Update Advisory - July 2021 | N/A | www.oracle.com |
| Oracle Critical Patch Update Advisory - October 2021 | MISC | www.oracle.com |
| [SECURITY] Fedora 32 Update: c-ares-1.17.0-1.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] Fedora 32 Update: mingw-c-ares-1.17.1-1.fc32 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| [SECURITY] Fedora 33 Update: c-ares-1.17.0-1.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| c-ares: Denial of service (GLSA 202012-11) — Gentoo security | GENTOO | security.gentoo.org |
| [SECURITY] Fedora 32 Update: mingw-c-ares-1.17.1-1.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| NodeJS: Multiple vulnerabilities (GLSA 202101-07) — Gentoo security | GENTOO | security.gentoo.org |
| HackerOne | MISC | hackerone.com |
| [SECURITY] Fedora 32 Update: c-ares-1.17.0-1.fc32 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| Oracle Critical Patch Update Advisory - April 2021 | MISC | www.oracle.com |
| November 2020 Security Releases Node.js | CONFIRM | nodejs.org |
| Oracle Critical Patch Update Advisory - January 2021 | MISC | www.oracle.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376120](#) F5 BIG-IP Local Traffic Manager (LTM), Access Policy Manager (APM), Application Security Manager (ASM) Node.js Vulnerability (K07944249)

[377388](#) Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2021:0016)

[500438](#) Alpine Linux Security Update for nodejs

[501445](#) Alpine Linux Security Update for nodejs

| |
|---|
| 501638 Alpine Linux Security Update for nodejs-current |
| 504201 Alpine Linux Security Update for nodejs |
| 670384 EulerOS Security Update for c-ares (EulerOS-SA-2021-1941) |
| 670405 EulerOS Security Update for c-ares (EulerOS-SA-2021-1920) |
| 690151 Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (56ba4513-a1be-11eb-9072-d4c9ef517024) |
| 690355 Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (ad792169-2aa4-11eb-ab71-0022489ad614) |
| 750430 OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:0066-1) |
| 750432 OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:0064-1) |
| 750539 OpenSUSE Security Update for c-ares (openSUSE-SU-2020:2092-1) |
| 750553 OpenSUSE Security Update for c-ares (openSUSE-SU-2020:2045-1) |
| 900131 CBL-Mariner Linux Security Update for subversion 1.14.0 |
| 900132 CBL-Mariner Linux Security Update for c-ares 1.14.0 |
| 902831 Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (3922) |
| 908064 Common Base Linux Mariner (CBL-Mariner) Security Update for python-gevent (32281-1) |
| 940254 AlmaLinux Security Update for nodejs:14 (ALSA-2021:0551) |
| 940276 AlmaLinux Security Update for nodejs:12 (ALSA-2020:5499) |
| 960263 Rocky Linux Security Update for nodejs:12 (RLSA-2020:5499) |
| 960749 Rocky Linux Security Update for nodejs:14 (RLSA-2021:0551) |

© [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](#)