



CVE-2020-8265

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

Summary

CVE	CVE-2020-8265
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-06 21:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 are vulnerable to a use-after-free bug in its TLS implementation. \

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Oracle	Graalvm	19.3.4	All	All	All
Application	Oracle	Graalvm	20.3.0	All	All	All
Application	Oracle	Graalvm	19.3.4	All	All	All
Application	Oracle	Graalvm	20.3.0	All	All	All
Application	Siemens	Sinec Infrastructure Network Services	All	All	All	All

References

Reference	Source	Link	T
HackerOne	MISC	hackerone.com	E
[SECURITY] Fedora 33 Update: nodejs-14.15.4-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
January 2021 Security Releases Node.js	MISC	nodejs.org	V
January 2021 Node.js Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	T
Debian -- Security Information -- DSA-4826-1 nodejs	DEBIAN	www.debian.org	T
[SECURITY] Fedora 32 Update: nodejs-12.20.1-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: nodejs-14.15.4-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	M
NodeJS: Multiple vulnerabilities (GLSA 202101-07) — Gentoo security	GENTOO	security.gentoo.org	T
cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf	CONFIRM	cert-portal.siemens.com	
[SECURITY] Fedora 32 Update: nodejs-12.20.1-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	M
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle.com	T
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [199763](#) Ubuntu Security Notification for Node.js Vulnerabilities (USN-6380-1)
- [375337](#) IBM Spectrum Control Multiple Vulnerability(6415993)
- [377388](#) Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2021:0016)
- [500438](#) Alpine Linux Security Update for nodejs
- [501446](#) Alpine Linux Security Update for nodejs
- [501639](#) Alpine Linux Security Update for nodejs-current
- [504202](#) Alpine Linux Security Update for nodejs
- [690397](#) Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (08b553ed-537a-11eb-be6e-0022489ad614)
- [750420](#) OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:0082-1)
- [750430](#) OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:0066-1)
- [750431](#) OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:0065-1)
- [750432](#) OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:0064-1)
- [940231](#) AlmaLinux Security Update for nodejs:10 (ALSA-2021:0548)
- [940253](#) AlmaLinux Security Update for nodejs:12 (ALSA-2021:0549)

[940254](#) AlmaLinux Security Update for nodejs:14 (ALSA-2021:0551)

[960749](#) Rocky Linux Security Update for nodejs:14 (RLSA-2021:0551)

[960803](#) Rocky Linux Security Update for nodejs:12 (RLSA-2021:0549)

[960843](#) Rocky Linux Security Update for nodejs:10 (RLSA-2021:0548)

© [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](#)