



# CVE-2020-8287

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

## Summary

<b>CVE</b>	CVE-2020-8287
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-06 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 allow two copies of a header field in an HTTP request (for example

## Risk And Classification

### Problem Types: CWE-444

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	19.3.4	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	20.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	19.3.4	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	20.3.0	All	All	All
Application	<a href="#">Siemens</a>	<a href="#">Sinec Infrastructure Network Services</a>	All	All	All	All

## References

Reference	Source	Link	T
HackerOne	MISC	<a href="https://hackerone.com">hackerone.com</a>	E
[SECURITY] Fedora 33 Update: nodejs-14.15.4-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
January 2021 Security Releases   Node.js	MISC	<a href="https://nodejs.org">nodejs.org</a>	V
January 2021 Node.js Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	T
Debian -- Security Information -- DSA-4826-1 nodejs	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	T
[SECURITY] Fedora 32 Update: nodejs-12.20.1-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 3224-1] http-parser security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
[SECURITY] Fedora 33 Update: nodejs-14.15.4-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	M
NodeJS: Multiple vulnerabilities (GLSA 202101-07) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	T
<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf">cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf</a>	CONFIRM	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	
[SECURITY] Fedora 32 Update: nodejs-12.20.1-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	T
Oracle Critical Patch Update Advisory - January 2021	MISC	<a href="https://www.oracle.com">www.oracle.com</a>	T
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	c
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	c

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[181294](#) Debian Security Update for http-parser (DLA 3224-1)

[198898](#) Ubuntu Security Notification for http-parser Vulnerability (USN-5563-1)

[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)

[750383](#) OpenSUSE Security Update for nodejs8 (openSUSE-SU-2021:0195-1)

[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](#)**