



# CVE-2019-15605

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

## Summary

<b>CVE</b>	CVE-2019-15605
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-02-07 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:05:00 UTC
<b>Description</b>	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed

## 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="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	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
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	19.3.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	20.0.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All

## References

Reference	Source	Link	Tag
[SECURITY] Fedora 31 Update: libuv-1.34.2-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
Debian -- Security Information -- DSA-4669-1 nodejs	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
[security-announce] openSUSE-SU-2020:0293-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Node v10.19.0 (LTS)   Node.js	CONFIRM	<a href="https://nodejs.org">nodejs.org</a>	Rel
Oracle Critical Patch Update Advisory - July 2021	N/A	<a href="http://www.oracle.com">www.oracle.com</a>	
HackerOne	MISC	<a href="https://hackerone.com">hackerone.com</a>	Per
February 2020 Node.js Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
[SECURITY] Fedora 30 Update: nghttp2-1.40.0-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
February 2020 Security Releases   Node.js	CONFIRM	<a href="https://nodejs.org">nodejs.org</a>	Ver
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
[SECURITY] Fedora 31 Update: libuv-1.34.2-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Mai
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
Node v13.8.0 (Current)   Node.js	CONFIRM	<a href="https://nodejs.org">nodejs.org</a>	Ver
[SECURITY] Fedora 30 Update: nghttp2-1.40.0-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Node v12.15.0 (LTS)   Node.js	CONFIRM	<a href="https://nodejs.org">nodejs.org</a>	Rel
Node.js: Multiple vulnerabilities (GLSA 202003-48) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
Oracle Critical Patch Update Advisory - April 2020	N/A	<a href="http://www.oracle.com">www.oracle.com</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	can

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

199763	Ubuntu Security Notification for Node.js Vulnerabilities (USN-6380-1)
296075	Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)
376876	Alibaba Cloud Linux Security Update for http-parser (ALINUX2-SA-2020:0026)
377166	Alibaba Cloud Linux Security Update for http-parser (ALINUX3-SA-2022:0055)
500435	Alpine Linux Security Update for nodejs
501096	Alpine Linux Security Update for nodejs-current
504198	Alpine Linux Security Update for nodejs
505094	Alpine Linux Security Update for nodejs-current
940003	AlmaLinux Security Update for nodejs:10 (ALSA-2020:0579)
940191	AlmaLinux Security Update for nodejs:12 (ALSA-2020:0598)
960732	Rocky Linux Security Update for nodejs:10 (RLSA-2020:0579)
960870	Rocky Linux Security Update for nodejs:12 (RLSA-2020:0598)

© [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](#)