



# CVE-2022-35256

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-35256
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-05 22:15:00 UTC
<b>Updated</b>	2023-05-12 13:30:00 UTC
<b>Description</b>	The llhttp parser in the http module in Node v18.7.0 does not correctly handle header fields that are not terminated with CL

## 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>	11.0	All	All	All
Application	<a href="#">Llhttp</a>	<a href="#">Llhttp</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="#">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="#">Siemens</a>	<a href="#">Sinec Ins</a>	All	All	All	All
Application	<a href="#">Siemens</a>	<a href="#">Sinec Ins</a>	1.0	-	All	All
Application	<a href="#">Siemens</a>	<a href="#">Sinec Ins</a>	1.0	sp1	All	All
Application	<a href="#">Siemens</a>	<a href="#">Sinec Ins</a>	1.0	sp2	All	All

## References

Reference	Source	Link	Tags
HackerOne	MISC	<a href="https://hackerone.com">hackerone.com</a>	
Debian -- Security Information -- DSA-5326-1 nodejs	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
cert-portal.siemens.com/productcert/pdf/ssa-332410.pdf	CONFIRM	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	

CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">160143</a> Oracle Enterprise Linux Security Update for nodejs (ELSA-2022-6963)
<a href="#">160144</a> Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2022-6964)
<a href="#">160211</a> Oracle Enterprise Linux Security Update for nodejs:18 (ELSA-2022-7821)
<a href="#">160231</a> Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2022-7830)
<a href="#">160410</a> Oracle Enterprise Linux Security Update for nodejs and nodejs-nodemon (ELSA-2023-0321)
<a href="#">181502</a> Debian Security Update for nodejs (DSA 5326-1)
<a href="#">182159</a> Debian Security Update for nodejs (CVE-2022-35256)
<a href="#">199926</a> Ubuntu Security Notification for Node.js Vulnerabilities (USN-6491-1)
<a href="#">240731</a> Red Hat Update for nodejs:16 (RHSA-2022:6964)
<a href="#">240732</a> Red Hat Update for nodejs (RHSA-2022:6963)
<a href="#">240747</a> Red Hat Update for rh-nodejs14-nodejs (RHSA-2022:7044)
<a href="#">240851</a> Red Hat Update for nodejs:14 (RHSA-2022:7830)
<a href="#">240857</a> Red Hat Update for nodejs:18 (RHSA-2022:7821)
<a href="#">241117</a> Red Hat Update for nodejs and nodejs-nodemon security (RHSA-2023:0321)
<a href="#">241304</a> Red Hat Update for nodejs:14 security (RHSA-2023:1533)
<a href="#">241341</a> Red Hat Update for nodejs:14 security (RHSA-2023:1742)
<a href="#">283356</a> Fedora Security Update for nodejs (FEDORA-2022-de515f765f)
<a href="#">283357</a> Fedora Security Update for nodejs (FEDORA-2022-52dec6351a)
<a href="#">283432</a> Fedora Security Update for nodejs (FEDORA-2022-1667f7b60a)
<a href="#">296098</a> Oracle Solaris 11.4 Support Repository Update (SRU) 52.132.2 Missing (CPUOCT2022)
<a href="#">355273</a> Amazon Linux Security Advisory for nodejs : ALAS2023-2023-084
<a href="#">502514</a> Alpine Linux Security Update for nodejs-current
<a href="#">502530</a> Alpine Linux Security Update for nodejs
<a href="#">502531</a> Alpine Linux Security Update for nodejs

504211 Alpine Linux Security Update for nodejs
753199 SUSE Enterprise Linux Security Update for nodejs16 (SUSE-SU-2022:3656-1)
753342 SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2022:3616-1)
753404 SUSE Enterprise Linux Security Update for nodejs16 (SUSE-SU-2022:3615-1)
753490 SUSE Enterprise Linux Security Update for nodejs14 (SUSE-SU-2022:3614-1)
753698 SUSE Enterprise Linux Security Update for nodejs18 (SUSE-SU-2023:0419-1)
904629 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (11578)
904753 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (11578-1)
940692 AlmaLinux Security Update for nodejs (ALSA-2022:6963)
940721 AlmaLinux Security Update for nodejs:16 (ALSA-2022:6964)
940740 AlmaLinux Security Update for nodejs:18 (ALSA-2022:7821)
940775 AlmaLinux Security Update for nodejs:14 (ALSA-2022:7830)
940906 AlmaLinux Security Update for nodejs and nodejs-nodemon (ALSA-2023:0321)
960403 Rocky Linux Security Update for nodejs:16 (RLSA-2022:6964)
960479 Rocky Linux Security Update for nodejs:18 (RLSA-2022:7821)
960517 Rocky Linux Security Update for nodejs and nodejs-nodemon (RLSA-2023:0321)
960543 Rocky Linux Security Update for nodejs (RLSA-2022:6963)
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](#)**