



# CVE-2018-12121

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

## Summary

<b>CVE</b>	CVE-2018-12121
<b>State</b>	PUBLIC
<b>Assigner</b>	cve-request@iojs.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-11-28 17:29:00 UTC
<b>Updated</b>	2022-09-06 17:54:00 UTC
<b>Description</b>	Node.js: All versions prior to Node.js 6.15.0, 8.14.0, 10.14.0 and 11.3.0: Denial of Service with large HTTP headers: By usir

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joyent	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	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	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	8.2	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link	Tags
Malformed Request	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VDB En
November 2018 Security Releases   Node.js	CONFIRM	<a href="http://nodejs.org">nodejs.org</a>	Patch, Vendor Advisory
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	
Node.js: Multiple vulnerabilities (GLSA 202003-48) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.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

[296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)

[377509](#) Alibaba Cloud Linux Security Update for http-parser (ALINUX2-SA-2019:0063)

[378150](#) Virtuozzo Linux Security Update for http-parser (VZLSA-2019:2258)

[500432](#) Alpine Linux Security Update for nodejs

[501095](#) Alpine Linux Security Update for nodejs-current

[504195](#) Alpine Linux Security Update for nodejs

[900064](#) CBL-Mariner Linux Security Update for nodejs 8.11.4

[903050](#) Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (4297)

© [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](http://status.cve.report)