CVE-2019-15606

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-15606
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-07 15:15:00 UTC
Updated	2022-10-05 20:47:00 UTC
Description	Including trailing white space in HTTP header values in Nodejs 10, 12, and 13 causes bypass of authorization based on hea

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Ed
Operating System	Debian	Debian Linux	10.0	All	All
Operating System	Debian	Debian Linux	10.0	All	All
Application	Nodejs	Node.js	All	All	All
Application	Nodejs	Node.js	All	All	All
Operating System	Opensuse	Leap	15.1	All	All
Operating System	Opensuse	Leap	15.1	All	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.4.0	All	All
Application	Oracle	Graalvm	19.3.1	All	All
Application	Oracle	Graalvm	20.0.0	All	All
Application	Oracle	Graalvm	19.3.1	All	All
Application	Oracle	Graalvm	20.0.0	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Adviso
Debian -- Security Information -- DSA-4669-1 nodejs	DEBIAN	www.debian.org	Third Party Adviso
[security-announce] openSUSE-SU-2020:0293-1: important: Security update	SUSE	lists.opensuse.org	Mailing List, Third
Node v10.19.0 (LTS) | Node.js	CONFIRM	nodejs.org	Release Notes, Ve
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
February 2020 Node.js Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third Party Adviso
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Adviso
February 2020 Security Releases | Node.js	CONFIRM	nodejs.org	Vendor Advisory
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Adviso
Node v13.8.0 (Current) | Node.js	CONFIRM	nodejs.org	Vendor Advisory
Node v12.15.0 (LTS) | Node.js	CONFIRM	nodejs.org	Release Notes, Ve
Node.js: Multiple vulnerabilities (GLSA 202003-48) — Gentoo security	GENTOO	security.gentoo.org	Third Party Adviso
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Adviso
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Adviso
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.com	Third Party Adviso
HackerOne	MISC	hackerone.com	Exploit, Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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)
- 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)