



CVE-2020-11080

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-11080 |
| State | PUBLIC |
| Assigner | security-advisories@github.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-06-03 23:15:00 UTC |
| Updated | 2023-11-07 03:14:00 UTC |
| Description | In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of |

Risk And Classification

Problem Types: CWE-707

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------|---------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Application | Nghttp2 | Nghttp2 | All | All | All | All |
| Application | Nghttp2 | Nghttp2 | 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 | Opensuse | Leap | 15.1 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Application | Oracle | Banking Extensibility Workbench | 14.3.0 | All | All | All |
| Application | Oracle | Banking Extensibility Workbench | 14.4.0 | All | All | All |

| | | | | | | |
|-------------|--------|----------------------------------|--------|-----|-----|-----|
| Application | Oracle | Banking Extensibility Workbench | 14.3.0 | All | All | All |
| Application | Oracle | Banking Extensibility Workbench | 14.4.0 | All | All | All |
| Application | Oracle | Blockchain Platform | All | All | All | All |
| Application | Oracle | Enterprise Communications Broker | 3.1.0 | All | All | All |
| Application | Oracle | Enterprise Communications Broker | 3.2.0 | All | All | All |
| Application | Oracle | Enterprise Communications Broker | 3.1.0 | All | All | All |
| Application | Oracle | Enterprise Communications Broker | 3.2.0 | All | All | All |
| Application | Oracle | Graalvm | 19.3.2 | All | All | All |
| Application | Oracle | Graalvm | 20.1.0 | All | All | All |
| Application | Oracle | Graalvm | 19.3.2 | All | All | All |
| Application | Oracle | Graalvm | 20.1.0 | All | All | All |
| Application | Oracle | Mysql | All | All | All | All |
| Application | Oracle | Mysql | All | All | All | All |
| Application | Oracle | Mysql | All | All | All | All |
| Application | Oracle | Mysql | All | All | All | All |
| Application | Oracle | Mysql | All | All | All | All |

References

| Reference | Source | Link | Tag |
|--|---------|---|------|
| Debian -- Security Information -- DSA-4696-1 nodejs | DEBIAN | www.debian.org | This |
| Earlier check for settings flood · nghttp2/nghttp2@f8da73b · GitHub | MISC | github.com | Pat |
| Oracle Critical Patch Update Advisory - July 2020 | MISC | www.oracle.com | This |
| Oracle Critical Patch Update Advisory - April 2022 | MISC | www.oracle.com | |
| [SECURITY] Fedora 31 Update: nghttp2-1.41.0-1.fc31 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| Implement max settings option · nghttp2/nghttp2@336a98f · GitHub | MISC | github.com | Pat |
| Oracle Critical Patch Update Advisory - October 2020 | MISC | www.oracle.com | This |
| Oracle Critical Patch Update Advisory - July 2021 | N/A | www.oracle.com | |
| [SECURITY] Fedora 33 Update: nodejs-14.15.1-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org | This |
| [SECURITY] [DLA 3621-1] nghttp2 security update | MLIST | lists.debian.org | |
| [SECURITY] Fedora 33 Update: nodejs-14.15.1-1.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| [security-announce] openSUSE-SU-2020:0802-1: critical: Security update f | SUSE | lists.opensuse.org | Ma |
| [SECURITY] Fedora 31 Update: nghttp2-1.41.0-1.fc31 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org | This |
| Denial of service: Overly large SETTINGS frames · Advisory · nghttp2/nghttp2 · GitHub | CONFIRM | github.com | Pat |
| Oracle Critical Patch Update Advisory - January 2021 | MISC | www.oracle.com | This |
| [SECURITY] [DLA 2786-1] nghttp2 security update | MLIST | lists.debian.org | |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|---|
| 174829 SUSE Enterprise Linux Security update for nghttp2 (SUSE-SU-2021:0930-1) |
| 174830 SUSE Enterprise Linux Security update for nghttp2 (SUSE-SU-2021:0931-1) |
| 174848 SUSE Enterprise Linux Security update for nghttp2 (SUSE-SU-2021:0930-1) |
| 174849 SUSE Enterprise Linux Security update for nghttp2 (SUSE-SU-2021:0931-1) |
| 174904 SUSE Enterprise Linux Security Update for nghttp2 (SUSE-SU-2021:0932-1) |
| 178839 Debian Security Update for nghttp2 (DLA 2786-1) |
| 199397 Ubuntu Security Notification for nghttp2 Vulnerability (USN-6142-1) |
| 296072 Oracle Solaris 11.4 Support Repository Update (SRU) 25.75.3 Missing (CPUJUL2020) |
| 375444 IBM Spectrum Control Node js Vulnerability(6261327) |
| 377148 Alibaba Cloud Linux Security Update for nghttp2 (ALINUX3-SA-2022:0101) |
| 500424 Alpine Linux Security Update for nghttp2 |
| 500436 Alpine Linux Security Update for nodejs |
| 501097 Alpine Linux Security Update for nodejs-current |
| 501444 Alpine Linux Security Update for nodejs |
| 504183 Alpine Linux Security Update for nghttp2 |
| 504199 Alpine Linux Security Update for nodejs |
| 6000281 Debian Security Update for nghttp2 (DLA 3621-1) |
| 750297 OpenSUSE Security Update for nghttp2 (openSUSE-SU-2021:0468-1) |
| 900120 CBL-Mariner Linux Security Update for nghttp2 1.33.0 |
| 902870 Common Base Linux Mariner (CBL-Mariner) Security Update for nghttp2 (1936) |
| 940104 AlmaLinux Security Update for nodejs:12 (ALSA-2020:2852) |
| 940199 AlmaLinux Security Update for nodejs:10 (ALSA-2020:2848) |
| 940239 AlmaLinux Security Update for nghttp2 (ALSA-2020:2755) |
| 960225 Rocky Linux Security Update for nghttp2 (RLSA-2020:2755) |

960354 Rocky Linux Security Update for nodejs:12 (RLSA-2020:2852)

960425 Rocky Linux Security Update for nodejs:10 (RLSA-2020:2848)

© [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](#)