



CVE-2019-16792

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-16792 |
| State | PUBLIC |
| Assigner | security-advisories@github.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-01-22 19:15:00 UTC |
| Updated | 2022-09-23 18:58:00 UTC |
| Description | Waitress through version 1.3.1 allows request smuggling by sending the Content-Length header twice. Waitress would hear |

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | E |
|------------------|----------------------------|--|---------|--------|---|
| Application | Agendaless | Waitress | All | All | A |
| Operating System | Debian | Debian Linux | 9.0 | All | A |
| Application | Oracle | Communications Cloud Native Core Network Function Cloud Native Environment | 1.10.0 | All | A |

References

| Reference | Source | Link | Tags |
|---|---------|--|----------|
| Upon receiving invalid Content-Length bail · Pylons/waitress@575994c · GitHub | MISC | github.com | Patch |
| [SECURITY] [DLA 3000-1] waitress security update | MLIST | lists.debian.org | |
| HTTP Request Smuggling: Content-Length Sent Twice · Advisory · Pylons/waitress · GitHub | CONFIRM | github.com | Third Pa |
| Oracle Critical Patch Update Advisory - April 2022 | MISC | www.oracle.com | |
| Waitress — waitress 2.0.0 documentation | MISC | docs.pylonsproject.org | Release |
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|---|
| 174724 SUSE Enterprise Linux Security update for python-waitress (SUSE-SU-2020:3269-1) |
| 179276 Debian Security Update for waitress (DLA 3000-1) |
| 296075 Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020) |
| 750599 OpenSUSE Security Update for python-waitress (openSUSE-SU-2020:1922-1) |
| 750606 OpenSUSE Security Update for python-waitress (openSUSE-SU-2020:1911-1) |

© [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](#)