



# CVE-2019-16789

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

## Summary

<b>CVE</b>	CVE-2019-16789
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-26 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:05:00 UTC
<b>Description</b>	In Waitress through version 1.4.0, if a proxy server is used in front of waitress, an invalid request may be sent by an attacker

## Risk And Classification

**Problem Types:** CWE-444

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Application	<a href="#">Agendaless</a>	<a href="#">Waitress</a>	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Cloud Native Core Network Function Cloud Native Environment</a>	1.10.0	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	15	All

## References

Reference	Source	Link
[SECURITY] [DLA 3000-1] waitress security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[SECURITY] Fedora 30 Update: python-waitress-1.4.3-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Merge pull request from GHSA-m5ff-3wj3-8ph4 · Pylons/waitress@11d9e13 · GitHub	MISC	<a href="https://github.com">github.com</a>
Oracle Critical Patch Update Advisory - April 2022	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
[SECURITY] Fedora 31 Update: python-waitress-1.4.3-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: python-waitress-1.4.3-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
<a href="https://github.com/aithub/advisorv-review/pull/14604">github.com/aithub/advisorv-review/pull/14604</a>	CONFIRM	<a href="https://github.com">aithub.com</a>

Waitress — waitress 2.0.0 documentation	MISC	<a href="https://docs.pylonsproject.org">docs.pylonsproject.o</a>
[SECURITY] Fedora 31 Update: python-waitress-1.4.3-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">174724</a> SUSE Enterprise Linux Security update for python-waitress (SUSE-SU-2020:3269-1)
<a href="#">179276</a> Debian Security Update for waitress (DLA 3000-1)
<a href="#">296075</a> Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)
<a href="#">501369</a> Alpine Linux Security Update for py3-waitress
<a href="#">750599</a> OpenSUSE Security Update for python-waitress (openSUSE-SU-2020:1922-1)
<a href="#">750606</a> OpenSUSE Security Update for python-waitress (openSUSE-SU-2020:1911-1)
<a href="#">983109</a> Python (pip) Security Update for waitress (GHSA-968f-66r5-5v74)

© [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](#)