



CVE-2020-5236

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

Summary

CVE	CVE-2020-5236
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-04 03:15:00 UTC
Updated	2020-02-06 18:46:00 UTC
Description	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a head

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Agendaless	Waitress	1.4.2	All	All	All
Application	Agendaless	Waitress	1.4.2	All	All	All

References

Reference	Source	Link	Tags
Merge pull request from GHSA-73m2-3pwg-5fgc · Pylons/waitress@6e46f9e · GitHub	MISC	github.com	Patch, Third Party A
Catastrophic backtracking in regex allows Denial of Service · Advisory · Pylons/waitress · GitHub	CONFIRM	github.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

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)

[983116](#) Python (pip) Security Update for waitress (GHSA-73m2-3pwg-5fgc)

© [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](#)