



CVE-2023-46136

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

Summary

CVE	CVE-2023-46136
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 18:17:00 UTC
Updated	2023-11-01 16:50:00 UTC
Description	Werkzeug is a comprehensive WSGI web application library. If an upload of a file that starts with CR or LF and then is follow

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Palletsprojects	Werkzeug	All	All	All	All

References

Reference

- Merge 3.0.x (#2801) · pallets/werkzeug@f3c803b · GitHub
- DoS: High resource usage when parsing multipart/form-data containing a large part with CR/LF character at the beginning · Advisory · pallets/
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 242530 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:7477)
- 242551 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:7610)
- 242578 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:7473)
- 242872 Red Hat Update for OpenStack Platform 17.1 (RHSA-2024:0214)

242877 Red Hat Update for OpenStack Platform 17.1 (RHSA-2024:0189)
503487 Alpine Linux Security Update for py3-werkzeug
506180 Alpine Linux Security Update for py3-werkzeug
755208 SUSE Enterprise Linux Security Update for python-Werkzeug (SUSE-SU-2023:4288-1)
770216 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:7477)
770219 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:7610)
770220 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:7473)
907655 Common Base Linux Mariner (CBL-Mariner) Security Update for python-werkzeug (31701)
907664 Common Base Linux Mariner (CBL-Mariner) Security Update for python-werkzeug (31701-1)
995725 Python (Pip) Security Update for werkzeug (GHSA-hrfv-mqp8-q5rw)

© [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](#)