



# CVE-2019-10906

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

## Summary

<b>CVE</b>	CVE-2019-10906
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-07 00:29:00 UTC
<b>Updated</b>	2023-11-07 03:02:00 UTC
<b>Description</b>	In Pallets Jinja before 2.10.1, str.format_map allows a sandbox escape.

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Application	<a href="#">Palletsprojects</a>	<a href="#">Jinja</a>	All	All	All	All
Application	<a href="#">Palletsprojects</a>	<a href="#">Jinja</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Software Collections</a>	1.0	All	All	All

## References

Reference	Source	Link
USN-4011-1: Jinja2 vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
Jinja 2.10.1 Security Release   The Pallets Projects	MISC	<a href="https://palletsprojects.com">palletsprojects.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
[security-announce] openSUSE-SU-2019:1395-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
USN-4011-2: Jinja2 vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[SECURITY] Fedora 28 Update: python-jinja2-2.10.1-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[SECURITY] Fedora 28 Update: python-jinja2-2.10.1-1.fc28 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 29 Update: python-jinja2-2.10.1-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[security-announce] openSUSE-SU-2019:1614-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] Fedora 29 Update: python-jinja2-2.10.1-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] Fedora 30 Update: python-jinja2-2.10.1-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] Fedora 30 Update: python-jinja2-2.10.1-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.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

[376924](#) Alibaba Cloud Linux Security Update for python-jinja2 (ALINUX3-SA-2022:0066)

[670238](#) EulerOS Security Update for python-jinja2 (EulerOS-SA-2021-1838)

[670672](#) EulerOS Security Update for python-jinja2 (EulerOS-SA-2021-2430)

[940037](#) AlmaLinux Security Update for python-jinja2 (ALSA-2019:1152)

[960684](#) Rocky Linux Security Update for python-jinja2 (RLSA-2019:1152)

[981329](#) Python (pip) Security Update for Jinja2 (GHSA-462w-v97r-4m45)

© [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](#)