



CVE-2019-11324

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

Summary

CVE	CVE-2019-11324
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-18 21:29:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	The urllib3 library before 1.24.2 for Python mishandles certain cases where the desired set of CA certificates is different from

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Application	Python	Urllib3	All	All	All	All
Application	Python	Urllib3	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 2686-1] python-urllib3 security update	MLIST	lists.debian.org
[SECURITY] [DLA 3610-1] python-urllib3 security update	MLIST	lists.debian.org
oss-security - Re: urllib3: adds system certificates to ssl_context	MLIST	www.openwall.com
USN-3990-1: urllib3 vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com

Red Hat Customer Portal	REDHAT	access.redhat.com
Comparing a6ec68a...1efadf4 · urllib3/urllib3 · GitHub	MISC	github.com
[SECURITY] Fedora 30 Update: python-pip-19.0.3-6.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[security-announce] openSUSE-SU-2019:2133-1: moderate: Security update f	SUSE	lists.opensuse.org
[SECURITY] Fedora 31 Update: python-pip-19.1.1-7.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Red Hat Customer Portal	REDHAT	access.redhat.com
[SECURITY] Fedora 31 Update: python-pip-19.1.1-7.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 30 Update: python-pip-19.0.3-6.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[security-announce] openSUSE-SU-2019:2131-1: moderate: Security update f	SUSE	lists.opensuse.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159655](#) Oracle Enterprise Linux Security Update for python27:2.7 (ELSA-2020-1605)
- [159668](#) Oracle Enterprise Linux Security Update for python27:2.7 security and bug fix update (ELSA-2019-3335)
- [178673](#) Debian Security Update for python-urllib3 (DLA 2686-1)
- [377534](#) Alibaba Cloud Linux Security Update for python-pip (ALINUX2-SA-2020:0030)
- [377557](#) Alibaba Cloud Linux Security Update for python27:2.7 (ALINUX3-SA-2022:0112)
- [6000046](#) Debian Security Update for python-urllib3 (DLA 3610-1)
- [670234](#) EulerOS Security Update for python-urllib3 (EulerOS-SA-2021-1842)
- [940120](#) AlmaLinux Security Update for python27:2.7 (ALSA-2020:1605)
- [940202](#) AlmaLinux Security Update for python27:2.7 (ALSA-2019:3335)
- [982225](#) Python (pip) Security Update for urllib3 (GHSA-mh33-7rrq-662w)

© [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