



CVE-2019-9948

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

Summary

CVE	CVE-2019-9948
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-23 18:29:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass pro

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	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	19.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Netapp	Active Iq Performance Analytics Services	-	All	All	All
Application	Netapp	Active Iq Performance Analytics Services	-	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	2.7.16	-	All	All
Application	Python	Python	2.7.16	-	All	All

Application	Python	Python	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Tus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	8.0	All	All	All

References

Reference

[SECURITY] [DLA 2280-1] python3.5 security update

[2.7] bpo-35907: Avoid file reading as disallowing the unnecessary URL scheme in urllib (GH-11842) by push0ebp · Pull Request #11842 · pyt

Red Hat Customer Portal

Pony Mail!

[security-announce] openSUSE-SU-2019:1273-1: important: Security update

Slackware Security Advisory - python Updates ≈ Packet Storm

[SECURITY] Fedora 29 Update: python3-3.7.4-1.fc29 - package-announce - Fedora Mailing-Lists

USN-4127-1: Python vulnerabilities | Ubuntu security notices | Ubuntu

Pony Mail!

Python: Multiple vulnerabilities (GLSA 202003-26) — Gentoo security

Issue 35907: [security][CVE-2019-9948] Unnecessary URL scheme exists to allow local_file:// reading file in urllib - Python tracker

[security-announce] openSUSE-SU-2019:1580-1: important: Security update

March 2019 Python Vulnerabilities in NetApp Products | NetApp Product Security

Bugtraq: [slackware-security] python (SSA:2019-293-01)

USN-4127-2: Python vulnerabilities | Ubuntu security notices | Ubuntu

Red Hat Customer Portal

[SECURITY] Fedora 29 Update: python3-3.7.4-1.fc29 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 1884-1] python 3.5 security update

[SECURITY] [DLA 1834-1] python2.7 security update

Python urllib CVE-2019-9948 Security Bypass Vulnerability

Red Hat Customer Portal

[SECURITY] Fedora 30 Update: python3-3.7.4-1.fc30 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal

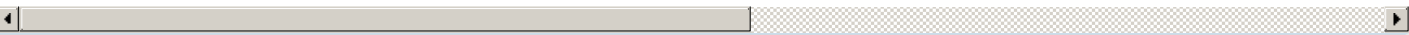
[SECURITY] [DLA 1852-1] python3.4 security update

[SECURITY] Fedora 30 Update: python3-3.7.4-1.fc30 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 2337-1] python2.7 security update

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159668](#) Oracle Enterprise Linux Security Update for python27:2.7 security and bug fix update (ELSA-2019-3335)

[296081](#) Oracle Solaris 11.4 Support Repository Update (SRU) 12.5.0 Missing (CPUJUL2019)

[376372](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Python Vulnerability (K28622040)

[377306](#) Alibaba Cloud Linux Security Update for python (ALINUX2-SA-2019:0094)

[377387](#) Alibaba Cloud Linux Security Update for python3 (ALINUX3-SA-2021:0080)

[500585](#) Alpine Linux Security Update for python2

[690721](#) Free Berkeley Software Distribution (FreeBSD) Security Update for python 3.6 (18ed9650-a1d6-11e9-9b17-fcaa147e860e)

[940202](#) AlmaLinux Security Update for python27:2.7 (ALSA-2019:3335)

© [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](#)