



CVE-2022-42919

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

Summary

CVE	CVE-2022-42919
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-07 00:15:00 UTC
Updated	2023-11-07 03:53:00 UTC
Description	Python 3.9.x before 3.9.16 and 3.10.x before 3.10.9 on Linux allows local privilege escalation in a non-default configuration.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All

References

Reference

- [SECURITY] Fedora 36 Update: python3.10-3.10.8-3.fc36 - package-announce - Fedora Mailing-Lists
- [SECURITY] Fedora 36 Update: pypy3.9-7.3.11-1.3.9.fc36 - package-announce - Fedora Mailing-Lists
- Comparing v3.10.8...v3.10.9 · python/cpython · GitHub
- [SECURITY] Fedora 37 Update: python3.9-3.9.15-2.fc37 - package-announce - Fedora Mailing-Lists
- [SECURITY] Fedora 35 Update: python3.10-3.10.8-3.fc35 - package-announce - Fedora Mailing-Lists
- [SECURITY] Fedora 37 Update: python3.10-3.10.8-3.fc37 - package-announce - Fedora Mailing-Lists
- CVE-2022-42919 Python Vulnerability in NetApp Products | NetApp Product Security
- [SECURITY] Fedora 35 Update: python3.10-3.10.8-3.fc35 - package-announce - Fedora Mailing-Lists

[\[SECURITY\] Fedora 35 Update: python3.9-3.9.15-2.fc35 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 36 Update: python3.9-3.9.15-3.fc36 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 37 Update: python3.9-3.9.15-2.fc37 - package-announce - Fedora Mailing-Lists](#)

[Python, PyPy3: Multiple Vulnerabilities \(GLSA 202305-02\) — Gentoo security](#)

[Linux specific local privilege escalation via the multiprocessing forserver start method - CVE-2022-42919 · Issue #97514 · python/cpython · GitHub](#)

[\[SECURITY\] Fedora 36 Update: pypy3.9-7.3.11-1.3.9.fc36 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 37 Update: pypy3.9-7.3.11-1.3.9.fc37 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 36 Update: python3.9-3.9.15-3.fc36 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 37 Update: python3.10-3.10.8-3.fc37 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 37 Update: pypy3.9-7.3.11-1.3.9.fc37 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 35 Update: python3.9-3.9.15-2.fc35 - package-announce - Fedora Mailing-Lists](#)

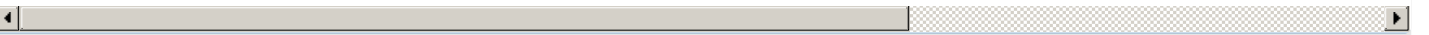
[\[SECURITY\] Fedora 36 Update: python3.10-3.10.8-3.fc36 - package-announce - Fedora Mailing-Lists](#)

[Comparing v3.9.15...v3.9.16 · python/cpython · GitHub](#)

[Linux specific local privilege escalation via the multiprocessing forserver start method - CVE-2022-42919 · Issue #97514 · python/cpython · GitHub](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160320](#) Oracle Enterprise Linux Security Update for python39:3.9 (ELSA-2022-8492)

[160324](#) Oracle Enterprise Linux Security Update for python3.9 (ELSA-2022-8493)

[183884](#) Debian Security Update for python3.11 (CVE-2022-42919)

[199016](#) Ubuntu Security Notification for Python Vulnerability (USN-5713-1)

[199497](#) Ubuntu Security Notification for Python Vulnerabilities (USN-5888-1)

[20342](#) Oracle Database 21c Critical Patch Update - April 2023

[240923](#) Red Hat Update for python39:3.9 (RHSA-2022:8492)

[240924](#) Red Hat Update for python3.9 (RHSA-2022:8493)

[283273](#) Fedora Security Update for python3.11 (FEDORA-2022-a04a020e48)

[283278](#) Fedora Security Update for python3.11 (FEDORA-2022-92ca0d5447)

[283321](#) Fedora Security Update for python3.9 (FEDORA-2022-1166a1df1e)

[283324](#) Fedora Security Update for python3.9 (FEDORA-2022-b17bf30e88)

283335 Fedora Security Update for python3.10 (FEDORA-2022-462f39dd2f)
283367 Fedora Security Update for python3.10 (FEDORA-2022-f44dd1bec2)
283427 Fedora Security Update for python3.9 (FEDORA-2022-028c09eaa7)
283428 Fedora Security Update for python3.10 (FEDORA-2022-a7cad6bd22)
283456 Fedora Security Update for python3 (FEDORA-2022-a9a4c48d06)
283600 Fedora Security Update for pypy3.9 (FEDORA-2023-af5206f71d)
283604 Fedora Security Update for pypy3.9 (FEDORA-2023-097dd40685)
284297 Fedora Security Update for python3.10 (FEDORA-2022-bd02afca8c)
284298 Fedora Security Update for python3.9 (FEDORA-2022-6728f16289)
354694 Amazon Linux Security Advisory for python3.9 : ALAS2022-2023-273
354708 Amazon Linux Security Advisory for python3.10 : ALAS2022-2023-274
355180 Amazon Linux Security Advisory for python3.9 : ALAS2023-2023-104
502608 Alpine Linux Security Update for python3
504338 Alpine Linux Security Update for python3
672677 EulerOS Security Update for python3 (EulerOS-SA-2023-1414)
672694 EulerOS Security Update for python3 (EulerOS-SA-2023-1429)
710714 Gentoo Linux Python, PyPy3 Multiple Vulnerabilities (GLSA 202305-02)
752899 SUSE Enterprise Linux Security Update for python39 (SUSE-SU-2022:4071-1)
753766 SUSE Enterprise Linux Security Update for python39 (SUSE-SU-2023:0707-1)
904479 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (11394)
904709 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (11394-1)
905381 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (13209)
906959 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (13209-1)
940781 AlmaLinux Security Update for python39:3.9 (ALSA-2022:8492)
940782 AlmaLinux Security Update for python3.9 (ALSA-2022:8493)
960186 Rocky Linux Security Update for python39:3.9 (RLSA-2022:8492)
960578 Rocky Linux Security Update for python3.9 (RLSA-2022:8493)

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](#)