



CVE-2021-23336

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

Summary

CVE	CVE-2021-23336
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-15 13:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	The package python/cpython from 0 and before 3.6.13, from 3.7.0 and before 3.7.10, from 3.8.0 and before 3.8.8, from 3.9.

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Djangoproject	Django	All	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Inventory Collect Tool	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Oracle	Communications Offline Mediation Controller	12.0.0.3.0	All	All	All
Application	Oracle	Communications Pricing Design Center	12.0.0.3.0	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0.0	All	All	All
Operating System	Oracle	Zfs Storage Appliance	8.8	All	All	All
Application	Python	Python	All	All	All	All

Application	Python	Python	All	All	All	All
References						
Reference						Source
[SECURITY] Fedora 33 Update: python2.7-2.7.18-11.fc33 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 34 Update: mingw-python3-3.9.2-2.fc34 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] [DLA 2619-1] python3.5 security update						MLIST
Pony Mail!						MLIST
[SECURITY] Fedora 32 Update: python3.10-3.10.0~a6-1.fc32 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 32 Update: mingw-python3-3.8.8-1.fc32 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 32 Update: mingw-python3-3.8.8-1.fc32 - package-announce - Fedora Mailing-Lists						
[SECURITY] Fedora 33 Update: python2.7-2.7.18-11.fc33 - package-announce - Fedora Mailing-Lists						
[SECURITY] Fedora 32 Update: python37-3.7.10-1.fc32 - package-announce - Fedora Mailing-Lists						
[SECURITY] Fedora 32 Update: python39-3.9.2-1.fc32 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 34 Update: python3.10-3.10.0~a6-1.fc34 - package-announce - Fedora Mailing-Lists						
[SECURITY] Fedora 32 Update: python37-3.7.10-1.fc32 - package-announce - Fedora Mailing-Lists						FEDORA
Pony Mail!						MLIST
[SECURITY] Fedora 32 Update: python3-3.8.9-1.fc32 - package-announce - Fedora Mailing-Lists						
[SECURITY] Fedora 33 Update: python3.10-3.10.0~a6-1.fc33 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 34 Update: python-django-3.1.7-1.fc34 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 32 Update: python-django-3.0.13-1.fc32 - package-announce - Fedora Mailing-Lists						
[SECURITY] Fedora 33 Update: python3.9-3.9.2-1.fc33 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 32 Update: python36-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists						
oss-security - Django security releases: CVE-2021-23336: Web cache poisoning via ``django.utils.http.limited_parse_qs()``						MLIST
Oracle Critical Patch Update Advisory - July 2021						N/A
[announce] 20210501 Apache Airflow CVE: CVE-2021-28359: Apache Airflow Reflected XSS via Origin Query Argument in URL						
[SECURITY] Fedora 34 Update: python3.10-3.10.0~a6-1.fc34 - package-announce - Fedora Mailing-Lists						FEDORA
Oracle Critical Patch Update Advisory - October 2021						MISC
[SECURITY] Fedora 33 Update: python-django-3.0.13-1.fc33 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 33 Update: python3.8-3.8.8-1.fc33 - package-announce - Fedora Mailing-Lists						FEDORA
Oracle Critical Patch Update Advisory - January 2022						MISC
oss-security - CVE-2021-28359: Apache Airflow Reflected XSS via Origin Query Argument in URL						MLIST
[SECURITY] Fedora 32 Update: python-django-3.0.13-1.fc32 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] [DLA 2569-1] python-django security update						MLIST
[SECURITY] Fedora 34 Update: python2.7-2.7.18-11.fc34 - package-announce - Fedora Mailing-Lists						FEDORA
[SECURITY] Fedora 34 Update: python3.10-3.10.0~a6-1.fc34 - package-announce - Fedora Mailing-Lists						FEDORA

[SECURITY] Fedora 33 Update: mingw-python3-3.9.2-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 32 Update: python39-3.9.2-1.fc32 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 33 Update: python3.6-3.6.13-1.fc33 - package-announce - Fedora Mailing-Lists	
[SECURITY] [DLA 2628-1] python2.7 security update	MLIST
[SECURITY] Fedora 32 Update: python36-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA
Pony Mail!	MLIST
[SECURITY] [DLA 3575-1] python2.7 security update	MLIST
[SECURITY] Fedora 33 Update: python3.7-3.7.10-1.fc33 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 33 Update: python3.8-3.8.8-1.fc33 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 34 Update: python2.7-2.7.18-11.fc34 - package-announce - Fedora Mailing-Lists	
Python: Multiple vulnerabilities (GLSA 202104-04) — Gentoo security	GENTOO
[SECURITY] Fedora 34 Update: mingw-python3-3.9.2-2.fc34 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 33 Update: mingw-python3-3.9.2-1.fc33 - package-announce - Fedora Mailing-Lists	
Web Cache Poisoning in python/cpython Snyk	MISC
[SECURITY] Fedora 32 Update: python3.10-3.10.0~a6-1.fc32 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 33 Update: python3.10-3.10.0~a6-1.fc33 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 33 Update: python3.6-3.6.13-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 32 Update: python3-3.8.9-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 33 Update: python-django-3.0.13-1.fc33 - package-announce - Fedora Mailing-Lists	
bpo-42967: only use '&' as a query string separator by AdamGold · Pull Request #24297 · python/cpython · GitHub	MISC
[SECURITY] Fedora 33 Update: python3.7-3.7.10-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA
[mina-dev] 20210225 [jira] [Created] (FTPSERVER-500) Security vulnerability in common/lib/log4j-1.2.17.jar	
Oracle Critical Patch Update Advisory - April 2021	MISC
CVE-2021-23336 Python Vulnerability in NetApp Products NetApp Product Security	CONFIRM
[SECURITY] Fedora 34 Update: python-django-3.1.7-1.fc34 - package-announce - Fedora Mailing-Lists	
[airflow-users] 20210501 CVE-2021-28359: Apache Airflow Reflected XSS via Origin Query Argument in URL	
[SECURITY] Fedora 33 Update: python3.9-3.9.2-1.fc33 - package-announce - Fedora Mailing-Lists	
Cache poisoning in popular open source packages Snyk Blog	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Snyk Security Team

159200 Oracle Enterprise Linux Security Update for python3 (ELSA-2021-1633)
159463 Oracle Enterprise Linux Security Update for python27:2.7 (ELSA-2021-4151)
159467 Oracle Enterprise Linux Security Update for python38:3.8 and python38-devel:3.8 (ELSA-2021-4162)
174803 SUSE Enterprise Linux Security update for python (SUSE-SU-2021:0768-1)
174820 SUSE Enterprise Linux Security update for python3 (SUSE-SU-2021:0886-1)
174825 SUSE Enterprise Linux Security update for python36 (SUSE-SU-2021:0887-1)
174842 SUSE Enterprise Linux Security update for python3 (SUSE-SU-2021:0947-1)
174861 SUSE Enterprise Linux Security Update for python3 (SUSE-SU-2021:0947-1)
178536 Debian Security Update for python3.5 (DLA 2619-1)
178546 Debian Security Update for python2.7 (DLA 2628-1)
180273 Debian Security Update for python3.9pypy3python-django (CVE-2021-23336)
181172 Debian Security Update for python-django (DLA 3164-1)
239323 Red Hat Update for python3 (RHSA-2021:1633)
239580 Red Hat Update for rh-python38 (RHSA-2021:3254)
239582 Red Hat Update for python27 (RHSA-2021:3252)
239826 Red Hat Update for python27:2.7 (RHSA-2021:4151)
239845 Red Hat Update for python38:3.8 and python38-devel:3.8 (RHSA-2021:4162)
281120 Fedora Security Update for python2.7 (FEDORA-2021-12df7f7382)
281121 Fedora Security Update for python2.7 (FEDORA-2021-98720f3785)
281358 Fedora Security Update for python3 (FEDORA-2021-b6b6093b3a)
281531 Fedora Security Update for mingw (FEDORA-2021-309bc2e727)
281532 Fedora Security Update for mingw (FEDORA-2021-b76ede8f4d)
281533 Fedora Security Update for mingw (FEDORA-2021-e525e48886)
281542 Fedora Security Update for python (FEDORA-2021-ef83e8525a)
281543 Fedora Security Update for python (FEDORA-2021-1bb399a5af)
281544 Fedora Security Update for python (FEDORA-2021-e22bb0e548)
281547 Fedora Security Update for python3.10 (FEDORA-2021-2897f5366c)
281548 Fedora Security Update for python3.10 (FEDORA-2021-5a09621ebb)

281549 Fedora Security Update for python3.10 (FEDORA-2021-b326fcb83f)
281604 Fedora Security Update for python3.9 (FEDORA-2021-b1843407ca)
281609 Fedora Security Update for python3.6 (FEDORA-2021-7fa9dc84d4)
352278 Amazon Linux Security Update for python35: ALAS-2021-1498
352305 Amazon Linux Security Advisory for python36: ALAS-2021-1500
352365 Amazon Linux Security Advisory for python34: ALAS-2021-1504
352371 Amazon Linux Security Advisory for python3: ALAS2-2021-1640
353942 Amazon Linux Security Advisory for python : ALAS2-2022-1802
353955 Amazon Linux Security Advisory for python27 : ALAS-2022-1593
375537 Python Buffer Overflow/Web Cache Poisoning Vulnerability
377387 Alibaba Cloud Linux Security Update for python3 (ALINUX3-SA-2021:0080)
500595 Alpine Linux Security Update for python3
501677 Alpine Linux Security Update for py3-django
504345 Alpine Linux Security Update for python3
6000148 Debian Security Update for python2.7 (DLA 3575-1)
670241 EulerOS Security Update for python (EulerOS-SA-2021-1835)
670313 EulerOS Security Update for python (EulerOS-SA-2021-1911)
670338 EulerOS Security Update for python3 (EulerOS-SA-2021-1886)
670368 EulerOS Security Update for python3 (EulerOS-SA-2021-1957)
670389 EulerOS Security Update for python3 (EulerOS-SA-2021-1936)
670668 EulerOS Security Update for python (EulerOS-SA-2021-2427)
710014 Gentoo Linux Python Multiple Vulnerabilities (GLSA 202104-04)
750307 OpenSUSE Security Update for python (openSUSE-SU-2021:0435-1)
900046 CBL-Mariner Linux Security Update for python3 3.7.9
900925 Common Base Linux Mariner (CBL-Mariner) Security Update for python2 (6827-1)
903306 Common Base Linux Mariner (CBL-Mariner) Security Update for python2 (3910)
903651 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (3911)
940187 AlmaLinux Security Update for python3 (ALSA-2021:1633)
940500 AlmaLinux Security Update for python3 (ALSA-2021:1454)

[940522](#) AlmaLinux Security Update for python27:2.7 (ALSA-2021:4151)

[940526](#) AlmaLinux Security Update for python38:3.8 and python38-devel:3.8 (ALSA-2021:4162)

[960320](#) Rocky Linux Security Update for python27:2.7 (RLSA-2021:4151)

[960342](#) Rocky Linux Security Update for python38:3.8 and python38-devel:3.8 (RLSA-2021:4162)

© [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](#)