



# CVE-2022-34265

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

## Summary

<b>CVE</b>	CVE-2022-34265
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-07-04 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:48:00 UTC
<b>Description</b>	An issue was discovered in Django 3.2 before 3.2.14 and 4.0 before 4.0.6. The Trunc() and Extract() database functions are

## Risk And Classification

### Problem Types: CWE-89

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Djangoproject	Django	All	All	All	All

## References

Reference	Source	Link
Redirecting to Google Groups		<a href="https://groups.google.com">groups.google.com</a>
Redirecting to Google Groups	MISC	<a href="https://groups.google.com">groups.google.com</a>
[SECURITY] Fedora 38 Update: python-django-4.0.10-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Django security releases issued: 4.0.6 and 3.2.14   Weblog   Django	CONFIRM	<a href="https://www.djangoproject.com">www.djangoproject.com</a>
Archive of security issues   Django documentation   Django	MISC	<a href="https://docs.djangoproject.com">docs.djangoproject.com</a>
CVE-2022-34265 Django Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
[SECURITY] Fedora 37 Update: python-django-4.0.10-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 38 Update: python-django-4.0.10-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 37 Update: python-django-4.0.10-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-5254-1 python-django	DEBIAN	<a href="https://www.debian.org">www.debian.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

181137	Debian Security Update for python-django (DSA 5254-1)
181172	Debian Security Update for python-django (DLA 3164-1)
184538	Debian Security Update for python-django (CVE-2022-34265)
198847	Ubuntu Security Notification for Django Vulnerability (USN-5501-1)
240925	Red Hat Update for Satellite 6.12 (RHSA-2022:8506)
283945	Fedora Security Update for python (FEDORA-2023-8fed428c5e)
284167	Fedora Security Update for python (FEDORA-2023-a53ab7c969)
296083	Oracle Solaris 11.4 Support Repository Update (SRU) 49.126.2 Missing (CPUOCT2022)
502440	Alpine Linux Security Update for py3-django
505305	Alpine Linux Security Update for py3-django
690891	Free Berkeley Software Distribution (FreeBSD) Security Update for django (5be19b0d-fb85-11ec-95cd-080027b24e86)
960485	Rocky Linux Security Update for Satellite (RLSA-2022:8506)

© [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](#)