



CVE-2020-25626

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-25626
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-30 20:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	A flaw was found in Django REST Framework versions before 3.12.0 and before 3.11.2. When using the browseable API vi

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Encode	Django Rest Framework	All	All	All	All
Application	Encode	Django Rest Framework	All	All	All	All
Application	Redhat	Ceph Storage	2.0	All	All	All
Application	Redhat	Ceph Storage	2.0	All	All	All

References

Reference	Source	Link
1878635 – (CVE-2020-25626) CVE-2020-25626 django-rest-framework: XSS Vulnerability in API viewer	MISC	bugzilla.redhat.com
CVE-2020-25626 Django Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Debian -- Security Information -- DSA-5186-1 djangorestframework	DEBIAN	www.debian.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

[180896](#) Debian Security Update for djangoestframework (DSA 5186-1)

[180897](#) Debian Security Update for djangoestframework (DSA 5186-1)

[750351](#) OpenSUSE Security Update for python-djangoestframework (openSUSE-SU-2021:0322-1)

[982897](#) Python (pip) Security Update for djangoestframework (GHSA-fx83-3ph3-9j2q)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)