CVE-2020-25626

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

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 djangorestframework (DSA 5186-1)

180897 Debian Security Update for djangorestframework (DSA 5186-1)

750351 OpenSUSE Security Update for python-djangorestframework (openSUSE-SU-2021:0322-1)

982897 Python (pip) Security Update for djangorestframework (GHSA-fx83-3ph3-9j2q)