



CVE-2018-25045

Published on: Not Yet Published

Last Modified on: 07/29/2022 03:31:00 AM UTC

CVE-2018-25045

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Django Rest Framework](#) from [Django-rest-framework](#) contain the following vulnerability:

Django REST framework (aka django-rest-framework) before 3.9.1 allows XSS because the default DRFBrowsable API view templates disable autoescaping.

CVE-2018-25045 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
Fix XSS caused by disabled autoescaping in the default DRFBrowsable API view templates by zyv · Pull Request #6330 · encode/django-rest-framework · GitHub	github.com text/html	MISC github.com/encode/django-rest-framework/pull/6330
Fix XSS caused by disabled autoescaping in the default DRFBrowsable ... · encode/django-rest-framework@4bb9a3c · GitHub	github.com text/html	MISC github.com/encode/django-rest-framework/commit/4bb9a3c48427867ef1e46f7dee945a4c25a4f9b8
Problem: autoescape not getting passed to urlize_quoted_links filter by dkliban · Pull Request #6191 · encode/django-rest-framework · GitHub	github.com text/html	MISC github.com/encode/django-rest-framework/pull/6191

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

CVE.report does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Django-rest-framework	Django Rest Framework	All	All	All	All
cpe:2.3:a:django-rest-framework:django_rest_framework.*.*.*.*.*.*.*.*.*.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)