



CVE-2021-25986

Published on: 11/23/2021 12:00:00 AM UTC

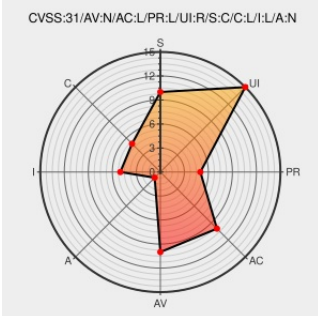
Last Modified on: 11/29/2021 04:07:00 PM UTC

CVE-2021-25986 - advisory for <https://www.whitesourcesoftware.com/vulnerability-database/>

Source: [Mitre](#)

Source: [Nist](#)

Print: [PDF](#)



Certain versions of [Django-wiki](#) from [Django-wiki Project](#) contain the following vulnerability:

In Django-wiki, versions 0.0.20 to 0.7.8 are vulnerable to Stored Cross-Site Scripting (XSS) in Notifications Section. An attacker who has access to edit pages can inject JavaScript payload in the title field. When a victim gets a notification regarding the changes made in the application, the payload in the notification panel renders and loads

external JavaScript.

CVE-2021-25986 has been assigned by vulnerabilitylab@whitesourcesoftware.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Django-wiki](#) - Django-wiki version $\geq 0.0.20$

Affected Vendor/Software: [Django-wiki](#) - Django-wiki version $\leq 0.7.8$



CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Security fix (XSS) - Build HTML elements for notifications safely · django-wiki/django-wiki@9eacc7 · GitHub	github.com text/html	 MISC github.com/django-wiki/django-wiki/commit/9eacc7519e4206a4d2f22640882f0737b2da9c5
CVE-2021-25986 WhiteSource Vulnerability Database	www.whitesourcesoftware.com text/html	 MISC www.whitesourcesoftware.com/vulnerability-database/CVE-2021-25986

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 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-wiki Project	Django-wiki	All	All	All	All

cpe:2.3:a:django-wiki_project:django-wiki:*:*:*:*:*:*:

Discovery Credit

WhiteSource Vulnerability Research Team (WVR)

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-25986 : In Django-wiki, versions 0.0.20 to 0.7.8 are vulnerable to Stored Cross-Site Scripting #XSS in N... twitter.com/i/web/status/1...	2021-11-23 19:20:38
 @LinInfoSec	Django - CVE-2021-25986: github.com/django-wiki/dj...	2021-11-23 21:36:13

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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](#)