



CVE-2025-13030

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

Summary

CVE	CVE-2025-13030
State	PUBLISHED
Assigner	snyk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 06:16:14 UTC
Updated	2026-04-30 06:16:14 UTC
Description	All versions of the package django-mdeditor are vulnerable to Missing Authentication for Critical Function in the image uplo

Risk And Classification

Primary CVSS: v4.0 2 LOW from report@snyk.io

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-306 | CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
4.0	report@snyk.io	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/E:P
3.1	report@snyk.io	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:L
3.1	CNA	DECLARED	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:L/E:P

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Django-mdeditor	affected * semver	Not specified

References

Reference	Source	Link	Tags
github.com/pylixm/django-mdeditor/commit/3e80f9edcabc5d2fc136b05a501964b...	report@snyk.io	github.com	
github.com/pylixm/django-mdeditor/pull/185	report@snyk.io	github.com	

github.com/pylixm/django-mdeditor/blob/e8dd73fb8571dfff2e7a20a4bfa88c376...	report@snyk.io	github.com	
github.com/pylixm/django-mdeditor/issues/151	report@snyk.io	github.com	
security.snyk.io/vuln/SNYK-PYTHON-DJANGOMDEDITOR-8630926	report@snyk.io	security.snyk.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Jeager Coder (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report