CVE-2017-6591

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

Summary

CVE	CVE-2017-6591
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-09 20:59:00 UTC
Updated	2017-03-21 01:59:00 UTC
Description	There is a cross-site scripting vulnerability in django-epiceditor 0.2.3 via crafted content in a form field.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Django-epiceditor Project	Django-epiceditor	0.2.3	All	All	All
Application	Django-epiceditor Project	Django-epiceditor	0.2.3	All	All	All

References

Reference	Source	Link	Tags
django-epiceditor CVE-2017-6591 Cross Site Scripting Vulnerability	BID	www.securityfocus.com	
Cross site scripting vulnerability in django-epiceditor | Morning Chen	MISC	morningchen.com	Exploit, Technical Description,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980783 Python (pip) Security Update for django-epiceditor (GHSA-xp5m-4c9f-498q)

Free CVE JSON API cve.report/api

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