



CVE-2011-0697

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

Summary

CVE	CVE-2011-0697
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-14 21:00:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in Django 1.1.x before 1.1.4 and 1.2.x before 1.2.5 might allow remote attackers to i

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Djangoproject	Django	1.1	All	All	All

Application	Djangoproject	Django	1.1.0	All	All	All
Application	Djangoproject	Django	1.1.2	All	All	All
Application	Djangoproject	Django	1.1.3	All	All	All
Application	Djangoproject	Django	1.2	All	All	All
Application	Djangoproject	Django	1.2.1	All	All	All
Application	Djangoproject	Django	1.2.2	All	All	All
Application	Djangoproject	Django	1.2.3	All	All	All
Application	Djangoproject	Django	1.2.4	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References			
Reference	Source		Link
[SECURITY] Fedora 14 Update: Django-1.2.5-1.fc14	af854a3a-2127-422b-91ae-364da2661108		lists.fe
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108		www.
676359 – (CVE-2011-0697) CVE-2011-0697 Django Potential XSS in file field rendering	af854a3a-2127-422b-91ae-364da2661108		bugzil
Webmail - OVH	af854a3a-2127-422b-91ae-364da2661108		www.
Webmail - OVH	af854a3a-2127-422b-91ae-364da2661108		www.
Debian update for python-django - Secunia.com	af854a3a-2127-422b-91ae-364da2661108		secur
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108		www.
Debian -- Security Information -- DSA-2163-1 python-django	af854a3a-2127-422b-91ae-364da2661108		www.
Django Multiple Vulnerabilities - Secunia.com	af854a3a-2127-422b-91ae-364da2661108		secur
Webmail - OVH	af854a3a-2127-422b-91ae-364da2661108		www.
Support / Security / Advisories // MDVSA-2011:031 Mandriva	af854a3a-2127-422b-91ae-364da2661108		www.
Ubuntu update for python-django - Secunia.com	af854a3a-2127-422b-91ae-364da2661108		secur
Django Weblog Security releases issued	af854a3a-2127-422b-91ae-364da2661108		www.
USN-1066-1: Django vulnerabilities Ubuntu	af854a3a-2127-422b-91ae-364da2661108		www.
[SECURITY] Fedora 13 Update: Django-1.2.5-1.fc13	af854a3a-2127-422b-91ae-364da2661108		lists.fe
Django Multiple Remote Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108		www.
oss-security - Django multiple flaws (CVEs inside)	af854a3a-2127-422b-91ae-364da2661108		openv
Fedora update for Django - Secunia.com	af854a3a-2127-422b-91ae-364da2661108		secur
CVE Program record	CVE.ORG		www.
NVD vulnerability detail	NVD		nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981192 Python (pip) Security Update for django (GHSA-8m3r-rv5g-fcpq)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)